WHAT PAYMENT INTERMEDIARIES ARE DOING ABOUT ONLINE LIABILITY AND WHY IT MATTERS

Mark MacCarthy†

† Adjunct Professor in the Communications Culture and Technology Program at Georgetown University. Formerly a Senior Vice President for Public Policy at Visa Inc.

I. INTRODUCTION

In the mid-1990s, commentators began debating the best way for governments to react to the development of the Internet as a global communications medium. Internet exceptionalists argued that the borderless nature of this new medium meant that the application of local law to online activities would create insoluble conflicts of law. The exceptionalists believed that as the Internet grew, 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 that should be ruled by norms developed by self-governing communities of users.[1]

Critics of the exceptionalist view responded with a vision of a bordered Internet where local governments could apply local law.[2] In this view, cyberspace is not a separate place. It is simply a communications network that links real people in real communities with other people in different jurisdictions. Governments can regulate activity on this new communications network in many different ways, including by relying on the local operations of global intermediaries. Global intermediaries are the internet service providers (ISPs), payment systems, search engines, auction sites, and other platform and application providers that provide the infrastructure necessary for internet activity. Although they are often global in character, they also have local operations subject to local government control. According to critics of the exceptionalist view, governments have the right and the obligation to use this regulatory power over intermediaries to protect their citizens from harm.[3] Conflicts that might arise from this regulatory activity can be resolved through the normal mechanisms governments use to resolve conflict of law questions.[4] Governments generally followed the advice of the proponents of regulation, not the regulatory skeptics.[5] And despite some set-backs in First Amendment cases,[6] regulators have continued a steady march

[1] *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1387–92 (1996).

[2] *E.g.*, Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

[3] *See id.* at 1238–39.

[4] *Id.* at 1200–01 (arguing that "regulation of cyberspace is feasible and legitimate from the perspective of jurisdiction and choice of law").

[5] The U.S. exception is § 230 of the Telecommunications Act of 1996 which immunizes many internet actors from liability in many contexts for the illegal activity of their users. 47 U.S.C. § 230(c) (2006).

[6] *See*, *e.g.*, Reno v. ACLU, 521 U.S. 844, 885 (1997) ("The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven

toward controlling the Internet by regulating intermediaries.[7] Some legal scholars argue that government reliance 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.[8] The key rationale is that governments cannot easily find wrongdoers on the Internet, but intermediaries can. They are in the best position to monitor their own systems. As Mann and Belzley put it, they are the "least-cost avoider."[9]

The defenders of local government jurisdiction over the Internet often rely on historical analogies to buttress their case that local control is inevitable and desirable. Debra Spar developed the thesis that society's reaction to new technologies follows a sequence of innovation, commercial exploitation, creative anarchy, and then government rules.[10] The four stages progress predictably: in the innovative stage, a new technology is developed; in the second stage, it is used in commercial ventures; in the third stage, 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 create and maintain the needed stability.[11] The development of radio is the standard example of this pattern. Radio's initial pioneers thought its ability to wirelessly broadcast information from one point to many made government control difficult and unnecessary.[12] But later commercial enterprises actively sought out government regulation in order to end the chaos on the airwaves that prevented broadcasters from reaching their intended audience.[13] Applying Spar's analysis here, the Internet is somewhere between stage three and stage four, where we can expect further regulation of internet activity under the watchful eye of government.

benefit of censorship."); Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 665 (E.D. Pa. 2004) (finding that a statute requiring ISPs to block access to websites displaying child pornography violated the First Amendment).

[7] *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006) (citing many examples of this trend). This Article documents further examples in which payment systems were induced by laws, regulations, pressure, and notions of corporate responsibility to take actions to control the illegal online behavior of people using their systems.

[8] *See, e.g.*, Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 249–50 (2005).

[9] *Id.* at 249.

[10] DEBORA L. SPAR, RULING THE WAVES: CYCLES OF DISCOVERY, CHAOS, AND WEALTH FROM THE COMPASS TO THE INTERNET 11–22 (2001).

[11] *Id.*; *see also* Mann & Belzley, *supra* note 8, at 243–44; GOLDSMITH & WU, *supra* note 7, at 124 (relying on Spar's work).

[12] *See generally* SPAR, *supra* note 10, at 124–90 (describing the history of radio technology development).

[13] *Id.* at 171–72.

The historical example demonstrates that although every new technology is thought to be outside the jurisdiction of government, this belief usually gives way in time to the realities of government control.

In the case of the Internet, the advent of government control prompted many observers to think the internet exceptionalists had been routed.[14] However, internet exceptionalism is still a widely held viewpoint,[15] and the notion that government control of cyberspace is both impossible and illegitimate still motivates much discussion of internet policy.[16] Moreover, the initial legislative expression of internet exceptionalism—§ 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 entities providing internet access service or online services.[17] Despite a growing call to revisit this immunity,[18] it has been extended several times. The internet gambling law, which creates liability for traditional intermediaries such as payment systems, contains a limitation on liability for pure internet intermediaries.[19] Similarly, the recently passed online

[14] *See* GOLDSMITH & WU, *supra* note 7, at 14 (asserting that "notions of a self-governing cyberspace are largely discredited").

[15] *See generally* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE (David Kairys ed., 2009) [hereinafter POST, IN SEARCH OF JEFFERSON'S MOOSE] (demonstrating an elegant take on internet exceptionalism). 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* David G. Post, *Against "Against Cyberanarchy"*, 17 BERKELEY TECH. L.J. 1365, 1384 (2002) [hereinafter Post, *Against "Against Cyberanarchy"*].

[16] *See* H. Brian Holland, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 U. KAN. L. REV. 369, 397 (2007). Holland's version of modified exceptionalism is closely connected with the legal principle that online intermediaries are not liable for third party conduct. He asserts that the immunity from liability created by § 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.

Id. at 397.

[17] 47 U.S.C. § 230(c)(1) (2006) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."). The interpretation of this provision is quite broad. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997) (finding that plaintiff's tort claims of defamation were preempted by § 230). The immunity does not extend to criminal law, contract law, or intellectual property law. 47 U.S.C. § 230(e)(1)–(4) (2006).

[18] *See, e.g.*, Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 U. CHI. SUP. CT. ECON. REV. 221 (2006).

[19] 31 U.S.C. § 5365(c) (2006).

pharmacy law exempts pure internet intermediaries from a general duty to avoid aiding or abetting unauthorized internet sales of controlled substances.[20] The adoption of these provisions in recent laws might be merely § 230 on automatic pilot, but more likely, some version of internet exceptionalism is at work in these legislative distinctions.

Given that parties on both sides of the internet exceptionalism debate can point to legislative manifestations of their arguments, it is clear that the question is far from fully settled. For these reasons, it is worth revisiting the intermediary liability debate in light of the experience that internet intermediaries have had in controlling internet content.

If the internet exceptionalists rested their case on the literal impossibility of extending local law to cyberspace, then there is not much left to their argument. A "bordered Internet" where intermediaries try to control behavior prohibited by local law is becoming a reality. Most internet intermediaries have explicit policies generally prohibiting them from aiding illegal activities.[21] These general policies are supplemented with specific policies and procedures designed to prevent the use of these systems for specific illegal activities. This Article focuses on the traditional payment intermediaries—payment card companies such as Visa, MasterCard, and American Express—as an instructive category of intermediary platforms. Developments over the last several years conclusively demonstrate that these payment intermediaries can control specific illegal activities on the Internet.

Thus, the debate over internet exceptionalism has rapidly shifted from the "nature" of the Internet as something intrinsically beyond the control of

---

[20] Ryan Haight Online Pharmacy Consumer Protection Act of 2008, Pub. L. No. 110-425, § (h)(3)(A)(iii), 122 Stat. 4829–30.

[21] 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." Google Inc. Advertising Program Terms 4 (Aug. 22, 2006), *available 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." MASTERCARD, MASTERCARD RULES 5.9.7 (2008), *available at* http://www.merchantcouncil.org/merchant-account/downloads/mastercard/MasterCard_Rules_5_08.pdf. MasterCard prohibits its issuing banks from engaging in illegal transactions. *Id.* at 3.8.4. 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." VISA, VISA INTERNATIONAL OPERATING REGULATIONS 4.1.B.1.c (2008), *available at* http://usa.visa.com/download/merchants/visa-international-operating-regulations.pdf. Visa's regulations also specify acquirer penalties for merchants engaging in illegal cross-border transactions. *Id.* at 1.6.D.16.

governments to a problem of choice.[22] Intermediaries can control illegal behavior on the Internet and governments can control intermediaries, but should they? And if governments should exert control over intermediaries, how should the global legal order be structured to accommodate their role?

The experiences of traditional payment intermediaries in acting to limit internet gambling, child pornography, controlled substances, online tobacco, and online copyright infringement provide a useful lens to address these questions. These payment intermediary practices suggest several lessons. 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, the decision to impose legal responsibilities on intermediaries should not be based on the least cost avoider principle. Assessments of intermediary liability must take into account market failures, as well as an analysis of costs, benefits, and equities. Third, exceptionalism is not the right framework for internet governance because intermediaries should not defer to the judgments of self-governing communities of internet users when these judgments conflict with local law. Fourth, the exceptionalists are right that a "bordered Internet" will not scale well. The experience of traditional payment systems points towards international harmonization. If governments are going to use intermediaries to regulate the Internet, they need to coordinate their laws to make that role possible.

Part II of this Article outlines a framework for analyzing intermediary liability. This framework calls for a thorough analysis, including an assessment of market failure and an examination of the costs, benefits, and equities involved in imposing intermediary liability. Part III applies this framework to the policies and practices of payment intermediaries in the areas of internet gambling, child pornography, controlled substances, online tobacco, and online copyright infringement. Revisiting the internet governance question, Part IV rejects the vision of a bordered Internet on the exceptionalist ground that it will not scale well. But despite the exceptionalist view, some form of internationalism is the best way forward.

II. INDIRECT INTERMEDIARY LIABILITY

A. INDIRECT LIABILITY REGIMES

This Section distinguishes indirect liability regimes from other ways of imposing obligations on intermediaries. The basic contrast is between legal schemes that hold intermediaries responsible solely for their own bad

[22] *See* Holland, *supra* note 16, at 376–77 ("In this context, exceptionalism became an objective to be pursued and protected as a matter of choice, rather than a natural state.").

behavior versus those that also make them responsible for the illegal behavior of people using their platforms. Since these indirect liability regimes are often controversial both in principle and in practice, this Section also develops a framework for analyzing them. It calls for a multipart analysis of market failure, costs, benefits, and equities before the imposition of intermediary liability.

Most legal regimes impose direct liability. In contrast, 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 responsibility to prevent the harmful conduct of the bad actor or to compensate the wronged party for the harm. In the case of copyright infringement, for example, the bad actor would be the infringer, the wronged party would be the record company that owned the music copyrights, and the third party would be an ISP or a payment system that facilitates the infringement.[23]

Indirect liability can be imposed through a variety of legal mechanisms.[24] 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. Statutes 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

[23] Indirect liability is not the same as holding a person responsible for the external negative effects of his own actions, but it bears a resemblance. With a negative externality, a person engages in some action, such as cattle-raising or industrial production, and the spillover 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.

[24] *See, e.g.*, Douglas Lichtman, *Holding Internet Service Providers Accountable*, 27 REG. 54, 59 (2004) (proposing that ISP liability for cyber security issues could be established in a regime of "negligence or strict liability, whether it is best implemented by statute or via gradual common law development"); Mann & Belzley, *supra* note 8, at 269–72 (suggesting three possible regimes: traditional tort regime, a takedown requirement, and a hot list).

requirements,[25] some privacy requirements,[26] and some consumer protection requirements imposed on financial service companies.[27]

---

[25] 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 associated with a breach when they failed to take specific precautions that are part of an industry data security standard. MINN. STAT. § 325E.64 (2009). Minnesota's law specifies that

> [n]o 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.

MINN. STAT. § 325E.64(2). This precaution of not saving authentication codes is based on the PCI DSS industry standard, Requirement 3.2. PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES VERSION 1.2.1 22 (July 2009), https://www.pci securitystandards.org/security_standards/pci_dss_download.html ("Do not store sensitive authentication data after authentication . . . ."). 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 . . . .

MINN. STAT. § 325E.64(3).

[26] 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 (e.g., by making sure that it is up to data and current, and by responding to data subject complaints of inaccuracy). This duty protects 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).

[27] 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 many of the same claims that they might assert against a merchant in connection with the purchase of defective or otherwise unsatisfactory goods and services; and the law limits a consumer's liability for unauthorized use of payment cards. *See* 15 U.S.C. § 1601 (2006) (regulating credit cards); 15 U.S.C. § 1693 (2006) (regulating debit 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

The current United States regime for intermediaries depends on the nature of the intermediary and the legal context. ISPs and some others enjoy substantial immunity.[28] The Communications Decency Act of 1996 exempted "interactive computer service providers" from certain kinds of third party liability by determining that they are not "the publisher or speaker of any information provided by another information content provider."[29] The Digital Millennium Copyright Act of 1998 (DMCA) 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.[30] The recent internet gambling and online pharmacy laws continue this tradition of immunity.[31]

Payment intermediaries are subject to an indirect liability regime by the provisions of the Unlawful Internet Gambling Enforcement Act (UIGEA).[32] Similarly, the new online pharmacy law might subject them to specific aiding or abetting liability for online sales of controlled substances.[33] But the Ninth

with cardholders in a payment system, and oblige financial institutions to protect cardholders from financial harms by fraudsters in connection with the fraudulent uses of payment cards. *See* 15 U.S.C. § 1601; 15 U.S.C. § 1693. The Truth in Lending Act (TILA), Pub. L. No. 90-321, 82 Stat. 146 (codified as amended at 15 U.S.C. § 1601 (2006)), was originally passed by Congress in 1968. Major amendments to the TILA were made by the Fair Credit Billing Act of 1974, Pub. L. No. 93-495, 88 Stat. 1511 (codified at 15 U.S.C. § 1666 (2006)), the Consumer Leasing Act of 1976, Pub. L. No. 94-240, 90 Stat. 257 (codified as amended at 15 U.S.C. § 1667 (2006)), and the Truth in Lending Simplification and Reform Act of 1980, Pub. L. No. 96-221, 94 Stat. 132. The Board of Governors of the Federal Reserve System implemented these requirements through Regulation Z. The implementation through Regulation Z is found in 12 C.F.R. § 226.12 (2009). The Electronic Fund Transfer Act, Pub. L. No. 95-630, 92 Stat. 3728 (codified at 15 U.S.C. § 1693 (2006)), was passed by Congress in 1978. The Board of Governors of the Federal Reserve System implemented these protections through Regulation E. 12 C.F.R. § 205 (2009). Regulation E does not provide redress to a consumer who has purchased allegedly defective goods or services using a debit card. *Id.*

[28] 47 U.S.C. § 230(c)(1) (2006); *see* Holland, *supra* note 16, at 373–76 (discussing the extension of this immunity).

[29] 47 U.S.C. § 230(c)(1).

[30] 17 U.S.C. § 512(a), (c)–(d) (2006).

[31] Unlawful Internet Gambling Enforcement Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (codified at 31 U.S.C. §§ 5361–5367 (2006)); Ryan Haight Online Pharmacy Consumer Protection Act of 2008, Pub. L. No. 110-425 §§ (h)(1)(B), (h)(2)(C), 122 Stat. 4820 (codified in 21 U.S.C. §§ 829, 802). This potential liability is discussed *infra* Sections III.A–III.B.

[32] Unlawful Internet Gambling Enforcement Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (codified at 31 U.S.C. §§ 5361–5367 (2006)).

[33] Ryan Haight Online Pharmacy Consumer Protection Act of 2008, Pub. L. No. 110-425 §§ (h)(1)(B), (h)(2)(C), 122 Stat. 4820; *see infra* Section III.B.2.

Circuit has held that payment intermediaries are not liable for copyright infringement on their systems.[34]

Online markets appear to be subject to some degree of indirect liability for the sale of counterfeit goods. The district court in *Tiffany (NJ) Inc. v. eBay, Inc.* held that eBay has some responsibilities under trademark law to avoid providing its services to sellers when it knows or has reason to know of trademark infringement by those sellers.[35] The online auction service satisfied that responsibility by implementing a series of measures including an effective voluntary notice-and-takedown system.[36] That responsibility did not extend, however, to a positive duty to monitor its auction site and preemptively remove possibly infringing listings.[37] The e-Fencing legislation, under consideration in the House of Representatives in 2009, would extend indirect liability for the sale of stolen goods to online markets.[38]

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.[39] A standard economic framework considers issues of market failure, costs and

---

[34] Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 795 (9th Cir. 2007).

[35] Tiffany (NJ) Inc. v. eBay, Inc., 576 F. Supp. 2d 463, 469–70 (S.D.N.Y. 2008).

[36] *Id.* at 478.

[37] The court held that eBay exerted sufficient control to be subjected to contributory liability, and then found that eBay's 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.

Id. at 470.

[38] E-Fencing Enforcement Act of 2009, H.R. 1166, 111th Cong. (2009) (requiring an online market provider to deny high volume sellers access to the marketplace if he has good reason to believe that the sellers acquired their goods unlawfully).

[39] *See generally* Lichtman & Posner, *supra* note 18 (summarizing this perspective); Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395, 396–99 (2003) (same as above).

benefits, and equity to assess the need for an indirect liability regime in specific cases.[40]

1. Market Failure Analysis

Before imposing an indirect liability regime, economic analysis asks whether there is really any market failure. If there is no market failure then, there is 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[41] and transaction costs are not significant.

Even if the wronged party cannot easily reach a bad actor that a third party can reach, it is still not necessary to impose liability on the third party. When the wronged party and the intermediary can easily negotiate an arrangement, efficiency will guide the third party to undertake 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.[42]

The presence of transaction costs deserves more emphasis. When a wronged party can directly deal with an involved third party to mitigate measurable financial harm, it is difficult to see why a third party liability rule matters from an efficiency point of view. No matter which party is liable, efforts to stop the harm should continue until further efforts are not worth it—until mitigation efforts cost more than they save. If liability is assigned to

---

[40] *See* Lichtman & Posner, *supra* note 18, at 228–33.

[41] The effective reach condition is evaluated prior to an assessment of the ability of a third party to effectively control the bad activity. *See id.* at 230–31. 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 could be 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 *infra*. Landes and Lichtman put the comparative point accurately, applied to the specific case of contributory copyright liability: "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 & Landes, *supra* note 39, at 398.

[42] Lichtman & Posner, *supra* note 18, at 235. Lichtman and Posner also focus 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 to ask how the parties would in that situation allocate responsibility for detecting and deterring bad acts." *Id.* at 257. 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.

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 pays. As Coase noted, the allocation of resources is the same, but the equities are different.[43]

In some cases, wronged parties bear the costs of these harms under today's legal regime.[44] 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 do not produce an equivalent reduction in damages.

The processes created by payment intermediaries to respond to external private party complaints reflect the beginnings of these arrangements and might develop into more productive relationships. The extensive processes used by eBay to police trademark violations are also the kind of measures that could be expanded to create efficient enforcement efforts.[45] However, mutually satisfactory enforcement arrangements involving third parties have not emerged to any large degree.[46]

This transaction cost perspective illuminates the issues at stake in *Tiffany (NJ) Inc. v. eBay, Inc.*[47] eBay has a notice-and-takedown program, described by a senior eBay official as follows:

---

[43] *See generally* Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960) (presenting the Coase theorem).

[44] This is simply the other side of the point that there is no universal rule of indirect liability for all harms.

[45] *See supra* notes 35–37 and accompanying text (discussing *Tiffany (NJ) Inc. v. eBay, Inc.*).

[46] *See, e.g.*, Lichtman & Posner, *supra* note 18, at 235–37 (expressing puzzlement as to why the parties have not worked out liability arrangements in their discussion of ISP liability for security flaws). 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 transaction costs are so high that intermediaries and wronged parties cannot reach efficient arrangements. It could mean that perceptions of equities prevent 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 112–13 (2004) (describing 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.

[47] 576 F. Supp. 2d 463 (S.D.N.Y. 2008).

> 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.[48]

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.[49] Instead, Tiffany wanted eBay to screen its customers, especially large volume customers, to check on whether their sale items were counterfeit. When these arrangements could not be worked out, Tiffany sued eBay for secondary trademark infringement.[50] But Tiffany could have offered to compensate eBay for the costs involved in the extra enforcement efforts it requested. There is no indication that transaction costs prevented negotiations.[51] The fact that eBay and Tiffany 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 it to take its own enforcement actions, the failure to reach an enforcement agreement suggests that eBay is not the least cost enforcer after all.[52]

---

[48] *Organized Retail Theft Prevention: Fostering a Comprehensive Public–Private Response: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 110th Cong. 26 (2007) (testimony of Robert Chesnut, Senior Vice President, Rules, Trust and Safety, eBay, Inc.).

[49] *eBay*, 576 F. Supp. 2d at 482 n.15.

[50] *Id.* at 469, 481–83.

[51] *See* Mann & Belzley, *supra* note 8, at 279 n.122. Mann and Belzley state,

> In a perfect world, the baseline would be irrelevant because the trademark owner would negotiate to purchase a takedown from eBay if that were an efficient outcome. Some reason exists to think that might happen where, as in this case, transaction costs between two large companies are low when compared to the value of the rights being negotiated.

Id.

[52] The *eBay* court 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.

576 F. Supp. 2d at 518. But if Tiffany thought that eBay could take enforcement action "more cheaply, quickly, and effectively than Tiffany," *id.*, why didn't they negotiate arrangements with eBay to do that? The fact that they didn't should be at least relevant

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.[53] eBay has an enforcement program called Partnering with Retailers Offensively Against Crime and Theft (PROACT)[54] and a mechanism to work with aggrieved merchants in connection with stolen merchandise.[55] 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.[56] If it seems that the item is stolen, eBay takes the item down, suspends the seller, and notifies law enforcement.[57] The contentious issue appears to be who should do the serious investigative work required in these cases. 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."[58] If all that is at stake is efficiency and not equity, and if 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 in which eBay undertakes these efforts on behalf of retailers.

A broader framework that accounts for equity and long-term intangible costs and benefits might provide a reason to impose third party liability even

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.

53 The House Judiciary Committee held a hearing on an earlier version of this legislation. To get a sense of how the proposed legislation might affect an online marketplace like eBay, see *E-fencing Enforcement of Act of 2008, the Organized Retail Crime Act of 2008, and the Combating Organized Retail Crime Act of 2008: Hearing on H.R. 6713, H.R. 6491 and S. 3434 Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 110th Cong. 32 (2008) [hereinafter *E-fencing Enforcement Hearing*] (statement of Edward Torpoco, Senior Regulatory Counsel, eBay, Inc.) (expressing concern that the bill would violate a fundamental legal principle that ISPs like eBay "should not be held liable for content posted by third parties").

54 PROACT allows retailers to submit reports to eBay's fraud investigators concerning suspected sales of stolen goods on eBay.

55 *E-fencing Enforcement Hearing*, *supra* note 53, at 27 (testimony of Edward Torpoco, Senior Regulatory Counsel, eBay, Inc.).

56 *Id.*

57 *Id.*

58 *Id.* at 46 (testimony of Joseph J. LaRocca, Vice President, Loss Prevention, National Retail Federation). It is hard to avoid the conclusion, voiced by Steve DelBianco on behalf of the online marketplaces at 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." *Id.* at 42 (testimony of Steve DelBianco, Executive Director, NetCHOICE).

when the parties can negotiate enforcement arrangements themselves. But the absence of such agreements in cases where parties can freely negotiate suggests that the wronged party does not think third party liability is worth paying for. This evaluation implied by the wronged party's actions should be a relevant factor taken into account in considering whether to impose third party liability.

The informal arrangements between law enforcement agencies and intermediaries with respect to specific illegal activities reflect the idea that parties can agree about who is responsible for enforcement even without any explicit indirect liability rules. Third parties have frequently worked closely with law enforcement to deter or prevent violations of the law. Intermediaries work with federal, state, and local law enforcement on a variety of issues, including fraud, child pornography, online tobacco sales, and controlled substances.[59] 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

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.[60] The first is the extent to which the third party is in a good position to detect or deter the illegal activity.[61] This is the "control" factor.[62] 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 all the third party's activity, legal and illegal alike.[63] This is the "activity" factor.[64] Both of these ideas apply traditional economic thinking to the special case of indirect liability rules.

The first factor—"control"—does not simply focus on whether the third party is in a good position to detect or deter the illegal activity. It also looks to whether the third party is in a better position than the wronged party, or other potentially liable third parties.[65] Through this analysis, the control factor reflects the "least cost" concept of third party liability.[66]

---

[59] *See infra* Section III.B.

[60] Lichtman & Posner, *supra* note 18, at 230–31.

[61] *Id.* at 230.

[62] *Id.*

[63] *Id.* at 231–32.

[64] *Id.*

[65] Several commentators seem to stop with the "good position" analysis. *See id.* at 223 ("Our argument in favor of service provider liability is primarily based on the notion that ISPs are in a good position to reduce the number and severity of bad acts online."); *see also*

A "least cost" perspective puts the burden of enforcing the law on the party that can stop the illegal transactions at the lowest cost. In the case of internet intermediaries, this line of thought can be summarized as follows: 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. In contrast, internet intermediaries possess 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. It thus seems efficient to adopt a legal rule assigning intermediaries the responsibility for stopping illegal internet transactions. As the least cost avoiders, they should be the internet police.[67]

Focusing on costs is desirable in order to create an efficient enforcement regime. 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, those costs will be passed down to their direct customers. 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 from an overall reduction in use also have to be counted.[68] According to the least cost idea, when these costs are less than the cost of enforcement activity by the wronged party or by enforcement officials, then liability rests with the intermediary.

Lichtman & Landes, *supra* note 39, at 409 (arguing regarding internet intermediaries that "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").

[66] There is an extensive law and economics literature in this area. *See, e.g.*, Mann & Belzley, *supra* note 8, at 265 (discussing the least-cost avoider principle); WARD FARNSWORTH, THE LEGAL ANALYST: A TOOLKIT FOR THINKING ABOUT THE LAW 47–56 (2007) (same as above).

[67] For the clearest argument in favor of intermediary liability based on this least cost avoider perspective, see Mann & Belzley, *supra* note 8, at 265.

[68] If there are fewer internet subscribers, then the service is less valuable to e-commerce merchants as well since there are fewer potential customers. *See* Matthew Schruers, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 250–52 (2002); *see also* Lichtman & Posner, *supra* note 18, at 241–43 (seeming to minimize the importance of these external, network effects in assessing liability regimes: "Immunizing ISPs from liability is not the correct mechanism for encouraging them to provide positive externalities."). However, the loss of 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's article gets the overall point right, noting: "To the extent the regulation affects conduct with positive social value, as is likely in at least some of the contexts this Article discusses, the direct and indirect effects on that conduct must be counted as costs of any regulatory initiative." Mann & Belzley, *supra* note 8, at 274.

This least cost avoider proposal is not advanced as an interpretation of current law.[69] In fact, some courts have explicitly repudiated this principle as an interpretation of current law.[70] 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 the third parties if the answer is affirmative.

But cost-based analysis is limited because it ignores the possibility that the benefits of enforcement efforts are less than the harm avoided. The mistake is to think that if efforts by third parties provide more enforcement than efforts by the wronged parties, then it must be worthwhile for the third parties to take these enforcement steps. Similarly, it is sometimes thought that if 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 almost always possible to spend more on enforcement and obtain some return. From an economic point of view, the question is whether that extra spending provides commensurate reductions in damages. Therefore, the least cost rule is not the right decision rule, even in a strictly economic analysis. Instead, a full cost-benefit analysis is more appropriate.[71]

This discussion of benefits is the appropriate context in which to analyze the "activity" factor described *infra*. Effort to reduce the harm facilitated by the third party imposes an external harm on someone else in the form of increased costs. Assigning liability to the third party for monetary damages for this harm means that the price of the activity it makes possible will rise, reducing all of the activity. This in effect internalizes the negative externality that these activities inflict on the wronged parties. Rather than just providing

---

[69] *See, e.g.*, Mann & Belzley, *supra* note 8, at 272. Mann and Belzley stated,

> The liability schemes that this Article envisions are plainly not the type of thing readily adopted through the development of the common law. This Article's frame-work is intended to provide fodder for legislators and regulators, not for judges. Hopefully, this Article's analysis can lead to well-specified statutory schemes or regulatory initiatives.

Id.

[70] *See, e.g.*, Tiffany (NJ) Inc. v. eBay, Inc., 576 F. Supp. 2d 463, 518 (S.D.N.Y. 2008) ("[E]ven 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.").

[71] 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. *See* Mann & Belzley, *supra* note 8, at 250 (adopting that perspective as "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.

the third party with an incentive to stop the harmful activity, the regulation of the intermediary discourages all of the activity it makes possible.[72]

The harm that intermediaries and the users of intermediary products and services would suffer from the imposition of an "activity" tax is an essential effect that 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, is justified only when the overall activity itself causes more harm than good. Following this approach in an effort to reduce online copyright infringement would require finding, 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 analysis helps assess the full cost of copyright enforcement: the price of additional copyright protection is that people will use internet services and applications less.[73]

A cost-benefit approach is often not considered in the case of general law enforcement because policymakers are reluctant to put a value on enforcement benefits. For example, policy makers may be unwilling to quantify the benefits of reduced child pornography or reduced sale of controlled substances. But in cases of more tangible harms, such as damages from copyright infringement or counterfeiting, a traditional cost-benefit analysis seems more feasible.

Cost-benefit analysis must take into account long-term considerations and dynamic conditions.[74] A version of the infant industry argument is also

---

[72] Lichtman & Posner, *supra* note 18, at 231; Lichtman & Landes, *supra* note 39, at 404–05 (illustrating how this "activity" factor works in discussing, "an instance where it would be prohibitively expensive to distinguish legal from illegal copyright activity," concluding that "Internet service providers are a good example in this category"). But then Lichtman and Landes 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.

Lichtman & Landes, *supra* note 39, at 405.

[73] It should be noted that Lichtman and Posner reject the activity factor rationale for imposing cyber-security liability on ISPs. Lichtman & Posner, *supra* note 18, at 238–40.

[74] *See* Lichtman & Landes, *supra* note 39, at 408. ("[L]ike any legal issue, these questions about the relative virtues of indirect liability have to be evaluated dynamically.").

relevant in this long-term context. Often industries need special help and consideration from government when they are just beginning. This help can take the form of public subsidies or immunities from normal legal liabilities. For example, the immunity from liability set out in § 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 internet infrastructure and services.[75]

A long-term analysis might consider what the world would look like if the same indirect liability burden was placed on third parties by other jurisdictions. It might also consider the likelihood that imposing liability in one case would cause other jurisdictions to also impose liability in other cases. The political implications are one aspect of this analysis. 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 consequences for the third party, which might potentially be burdened with costs from many jurisdictions—burdens that might be individually rational, but collectively unworkable. If the foreseeable result of imposing third party liability is 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 private parties involved and the costs and benefits to society. 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 the damage reduction but pays no costs. From an economic efficiency point of view, enforcement efforts that do not yield a commensurate reduction in damages are wasted. Private benefits may not be worth it from a social point of view when balanced against the costs to other parties.

3. Equity Analysis

The economic framework described above lacks a normative dimension. It does not take into account questions of fairness, rights, and justice. And it

[75] *See id.* at 406 (referencing this infant industry argument). *But see* Mann & Belzley, *supra* note 8, at 261 (appearing to be critical of the infant industry argument, 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").

does not consider who deserves the benefit of protection from harm or who is at fault, or blameworthy, for failing to take preventive measures. This Section points to the need to take these normative considerations into account.

Mann and Belzley take a strong position on this question and state that "a focus on traditional tort law notions of fault necessarily diverts attention to subjective normative questions of blame and responsibility . . . ."[76] The worry is that these notions will inevitably tangle up policy makers in difficult causation and responsibility questions and will divert attention from the key issue of who can fix the problem. The crucial factor for Mann and Belzley is not who created and maintains the problem, but who can fix it at the least cost.[77]

The view that an economic efficiency standard, by itself, is sufficient to create indirect liability is too strong. The focus on parties who had no part in creating the problem and who are not responsible for the illegal activity puts a burden on people who are innocent of any wrongdoing. Burdening innocent people seems unfair, and arguments that justify this approach on the grounds that it is good for society as a whole violate widely accepted moral principles and are unlikely to withstand public scrutiny.[78]

We should require 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 controversial in both moral and political philosophy.[79] Libertarians generally maintain that people need to fix only the problems that they themselves directly created.[80] Without this limitation, it is difficult not to slide into a

---

[76] Mann & Belzley, *supra* note 8, at 249. Mann and Belzley propose their idea, "liability without fault," to be that "intermediaries, without regard to their blame-worthiness, might be the most effective sources of regulatory enforcement." *Id.* at 262.

[77] Mann and Belzley also treat the least cost standard as a legal litmus test. *Id.* at 250–51. Being the least cost avoider is necessary and sufficient for indirect liability. No other standard or consideration intervenes to affect the analysis. As discussed, that standard leaves out the benefits part of the equation and is too limited.

[78] *See, e.g.*, JONATHAN WOLFF, AN INTRODUCTION TO POLITICAL PHILOSOPHY 57 (1996) (stating that "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 difficulty, but that approach is subject to difficulties of its own. *See generally* JOHN RAWLS, A THEORY OF JUSTICE (1971) (critiquing utilitarianism). The underlying intuition behind this alternative account of social justice is that "[e]ach person possesses an inviolability founded on justice that even the welfare of society as a whole cannot override." *Id.* at 3.

[79] *See infra* notes 80–83 and accompanying text.

[80] *See* Jim Harper, *Against ISP Liability*, 28 REG. 30, 30–31 (2005) (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

doctrine that requires all actors to stop misconduct whenever they can.[81] Others think that one has a duty to correct injustices to the extent that one participates in an institutional framework which produces injustice.[82] Still others believe in general positive duties to eliminate harms even when one has no direct role in causing them.[83]

Ultimately, the analysis of indirect liability cannot avoid considerations of fairness, rights, and justice. The key factors in this assessment will be those that have been used traditionally: directness of the involvement by third parties, an assessment of the degree of harm, the knowledge that third parties have or should have about the specific harm, third parties' intentions, whether the third parties are consciously acting in furtherance of a crime or other illegal act, and other similar considerations.[84] These complicated normative and empirical questions cannot be avoided by a single principle that purports to look at costs and benefits alone.[85]

---

not cause. *E.g.*, *id.*

[81] Mann & Belzley, *supra* note 8, at 272 (noting 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 possible" and finding that this "unbounded principle" is "unduly disruptive"). But it is hard to see how their proposal to implement indirect liability through regulation whenever it would be less expansive than leaving liability with the wronged party would be less disruptive.

[82] *See, e.g.*, THOMAS W. POGGE, WORLD POVERTY AND HUMAN RIGHTS 172 (2002) (arguing 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).

[83] *See, e.g.*, David Luban, *Just War and Human Rights*, *in* INTERNATIONAL ETHICS 195, 209 (Charles R. Beitz et al. eds., 1985) (stating that "all humans in a position to effect" a human right have an obligation to do so).

[84] Mann and Belzley criticize the "myopic focus on the idea that the inherent passivity of Internet intermediaries makes it normatively inappropriate to impose responsibility on them for the conduct of primary malfeasors." Mann & Belzley, *supra* note 8, at 261–62. But passivity is relevant to the knowledge and control factors needed to assess liability from an equity point of view. Lichtman and Landes 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." Lichtman & Landes, *supra* note 39, at 405. But these factors are crucial because they relate to the way in which the equity issues can be resolved.

[85] 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 are 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, should we not compensate the third party for taking the enforcement steps he is required to take? Assigning indirect liability when there is not this level of control or fault to justify blameworthiness might be so efficient under a cost analysis

There is another reason to consider equity. Even when transaction costs are low and parties can negotiate enforcement arrangements that make economic sense to them, it is still desirable to know whether it is fair, just, and equitable for one party to bear the cost. Distribution matters, not just efficiency. In fact, when courts decide cases where there are no apparent barriers to an efficient enforcement arrangement,[86] the major issues left are questions of equity.

Many who analyze indirect liability questions from an economic point of view recognize that non-economic factors also require consideration. Lichtman and Posner state that "[t]hese factors—call them 'control' and 'activity level'—help to identify cases where liability might be attractive. The actual question of whether liability should be imposed, however, typically turns on other, often setting-specific considerations."[87] 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.[88]

Because the economic argument is not sufficient on its own to justify indirect liability, it is usually supplemented with the language of blame. Judge Kozinski's 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.[89]

According to this argument, the intermediaries should be responsible for stopping the illegal activity, not simply because they are the least cost avoider, but because they profit from the illegal activity. There is a normative

that it is worth considering, but in that case the use of compensation mechanisms should also be considered.

[86] *See, e.g.*, Tiffany (NJ) Inc. v. eBay, Inc., 576 F. Supp. 2d 463 (S.D.N.Y. 2008).

[87] Lichtman & Posner, *supra* note 18, at 231.

[88] *Id.* at 231–32.

[89] Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 823 (9th Cir. 2007) (Kozinski, J., dissenting). Kozinski also states in his dissent that "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." *Id.* at 820. 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.

judgment here: people should not 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. Simultaneously, any efforts that the intermediary takes to mitigate the illegal activity are often downplayed or ignored, making it appear that the third party is willfully refusing to do his part.

This example's focus is not that normative considerations are inappropriate and so it would be better to limit the analysis to neutral economic analysis. Rather, the point 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.

III. APPLYING THE FRAMEWORK TO PAYMENT INTERMEDIARIES

Payment intermediaries have developed and refined policies and practices to deal with illegal internet transactions in their payment networks. This Part of the Article discusses several examples where these intermediaries took action to control illegal activity on their systems and applies the framework developed in Part II to these specific cases. This discussion illuminates some answers to the general question of the appropriate role of intermediaries in controlling illegal internet activity. For example, the internet gambling example illustrates the general point that intermediaries are better than others at monitoring their systems for activity of a certain type, but not for determining that these activities are illegal. Two general conclusions from this analysis are presented.

One conclusion that can be drawn from these examples is that payment intermediary action has been effective. As the following discussions demonstrate, internet gambling websites have been denied access to the U.S. market, and their current and projected revenues are in decline.[90] Websites for pornography, controlled substance, and tobacco have been substantially eliminated from the traditional payment systems.[91] Ongoing monitoring and enforcement actions in these areas continue to keep their presence in traditional payment networks at a minimal level.[92] For example, as a result of the payment system action in the Allofmp3.com copyright infringement case,

[90] *See infra* Section III.A.
[91] *See infra* Section III.B.
[92] *See infra* Section III.B.

Allofmp3.com was confined to a domestic market and experienced a dramatic reduction in the volume of activity at its website.[93]

The second conclusion from these examples is that the widespread assumption that payment system action in this area is simple and almost cost-free deserves more careful consideration.[94] The discussion of payment intermediaries' activities in the five case studies, infra, reveals substantial costs that should give policy makers pause before moving ahead with the imposition of an indirect liability scheme for payment providers. These include:

- The cost to maintain and enforce an internet gambling coding and blocking scheme that is entirely manual and cannot be automated;
- The cost from over-blocking legal transactions;
- The cost to screen and check the business activity of merchants participating in the payment systems;
- The cost to monitor the use of payment systems for specific illegal activity, where the payment systems are in no better position than anyone else to conduct this monitoring activity;
- The cost to assess complaints of illegality, where the intermediary has no special expertise and is often less familiar with the legal and factual issues than the wronged party and the allegedly bad actor;
- The cost to defend against legal challenges to enforcement actions, where the challenge typically comes in an off-shore jurisdiction; and
- Long-term costs to the United States from taking unilateral action in this area, including the encouragement of copycat regimes in other areas of law and in other jurisdictions.

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

Cost-benefit analysis can be labeled the enemy of regulation, but, 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

93 *See infra* Section III.C.3.

94 *See, e.g.*, *Perfect 10*, 494 F.3d at 824 (Kozinski, J., dissenting).

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. 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.

The payment intermediaries considered here 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 cards 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 who link separate financial institutions into an electronic payment network.[95]

These financial intermediaries are different from pure internet intermediaries. Pure internet intermediaries such as internet access providers, search engines, and online auction sites do not have a separate existence apart from the internet service or application that they provide.[96] Conversely, the traditional payment intermediaries evolved offline. The primary application of their services is face-to-face retail transactions, though they have extended this primary service to other channels such as mail-order and telephone service. The Internet is just another channel of commerce for them.[97] Despite this difference, their experiences controlling illegal online activity illuminate the general issue of intermediary liability for illegal online activity.

---

[95] 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 his or her account. 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. *See* DAVID S. EVANS & RICHARD SCHMALENSEE, PAYING WITH PLASTIC: THE DIGITAL REVOLUTION IN BUYING AND BORROWING 9–14 (2d ed. 2005) (further describing these payment systems).

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

[97] Payment intermediaries are similar to delivery services such as UPS or FedEx in this respect. They provide a service that is essential to the proper functioning of electronic commerce, but that service is not intrinsically tied to the online channel.

A. INTERNET GAMBLING LEGISLATION

The early efforts of government to use financial intermediaries to restrain internet gambling have been noted by other commentators.[98] These efforts came from state and federal law enforcement officials, who used their existing resources to pressure financial institutions to take steps against internet gambling merchants.[99] For example, Elliott Spitzer, then Attorney General for New York, pressured Citigroup and other financial institutions to agree to block internet gambling transactions in 2002.[100]

In 2006, Congress passed the Unlawful Internet Gambling Enforcement Act (UIGEA), which imposed a system of indirect liability on financial institutions for the purpose of preventing illegal internet gambling transactions.[101] At the time, many states made internet gambling illegal, and federal law outlawed at least some versions of it in interstate commerce.[102] But customers could evade these local laws by visiting internet gambling merchants located outside of the United States' jurisdiction. UIGEA was an attempt to enforce these local laws through the policies and practices of payment intermediaries.

Prior to the passage of UIGEA, payment card networks devised a coding and blocking system in order to manage the risks of internet gambling.[103] 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.[104] For gambling, this merchant category code was 7995.[105] In addition, merchants were required to use an electronic commerce indicator when an internet transaction was involved.[106] Together,

---

98 *See, e.g.*, Mann & Belzley, *supra* note 8, at 288–90.

99 *Id.*

100 GOLDSMITH & WU, *supra* note 7, at 82.

101 Unlawful Internet Gambling Enforcement Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (codified at 31 U.S.C. §§ 5361–5367 (2006)).

102 The Wire Act is used to prosecute internet gambling activities across state lines. 18 U.S.C. § 1084 (2006); *see also* U.S. GEN. ACCOUNTING OFFICE, INTERNET GAMBLING: AN OVERVIEW OF THE ISSUES 3–5 (2002) (describing the way these issues were perceived in 2002 when Congress was moving forward with internet gambling legislation).

103 *Financial Aspects of Internet Gaming: Good Gamble or Bad Bet?: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Financial Servs.*, 107th Cong. 25–27, 34–35 (2001) [hereinafter *Financial Aspects of Internet Gaming Hearing*] (statement and testimony of Mark MacCarthy, Senior Vice President, Public Policy, Visa, U.S.A., Inc.) (describing this system of coding and blocking internet gambling transactions); U.S. GEN. ACCOUNTING OFFICE, *supra* note 102, at 20–25 (same as above).

104 U.S. GEN. ACCOUNTING OFFICE, *supra* note 102, at 22.

105 VISA MERCHANT CATEGORY CLASSIFICATION (MCC) CODES DIRECTORY, *available at* http://www.da.usda.gov/procurement/card/card_x/mcc.pdf.

106 U.S. GEN. ACCOUNTING OFFICE, *supra* note 102, at 22.

these two pieces of information in the authorization message allowed payment networks or issuing banks to identify transactions involving internet gambling merchants.[107]

Given this system, it was entirely feasible for the issuing bank or the payment network to block internet gambling transactions. The system could accommodate conflicting laws in different jurisdictions 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 who permit internet gambling, such as the United Kingdom, could allow the use of their cards for internet gambling by not declining properly coded internet gambling transactions.

This system was a reasonable accommodation of 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. The British bank-issued card would work for internet gambling whereas the U.S. bank-issued card would not. People residing in countries where internet gambling was illegal were able to evade payment system blocking by obtaining cards issued by banks from jurisdictions where internet gambling was legal. This loophole was likely small and applied mostly to expatriates who did not give up their local cards when they moved to a new jurisdiction.

A second issue with the blocking system was that it could not accommodate legal gambling transactions made overseas by U.S. cardholders, who would find their cards declined for such activity. 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 detecting nuances in illegal versus legal internet gambling. If a jurisdiction recognized some internet gambling transactions as legal and others as illegal, the system would not detect it.[108] The merchant category code described a type of business, not the legal status of the transaction involved.[109] If a particular jurisdiction allowed casino gambling, but not sports betting, both transactions would nevertheless be labeled 7995. And if the system was set up to block these

---

[107] *Id.*

[108] U.S. GEN. ACCOUNTING OFFICE, *supra* note 102, at 22.

[109] *See* VISA MERCHANT CATEGORY CLASSIFICATION (MCC) CODES DIRECTORY, *supra* note 105 (listing all the MCC codes by "merchant type").

coded transactions, then both transactions, legal and illegal, would be blocked.[110]

Another weakness in the system was enforcement. If an internet gambling merchant realized that his transactions would be blocked in a large jurisdiction such as the United States, then he would have every incentive to hide.[111] Instead of describing itself as a gambling operation, the merchant would just code itself as a T-shirt sales site or some other legal entity. Without the proper merchant category code, the system was blind and could not effectively block the merchant's transactions.[112]

The payment networks addressed this enforcement issue with a special program to verify that internet gambling merchants coded their transactions correctly.[113] Payment network personnel would test transactions at popular internet gambling sites.[114] They would enter a transaction at the website and track the transaction through the payment system.[115] They would be able to tell whether the transaction was coded properly or not after they identified the transaction in the system.[116] If the transaction was not properly coded, the network would contact the bank that worked with the merchant and tell the bank that its merchant was out of compliance with the coding rule.[117] The payment network would ask the bank to take steps to bring the merchant into compliance.[118] Finally, the network would retest the site for proper coding.[119]

There was nothing automatic about the coding enforcement program. Staff manually entered the transactions, tracked them in the processing and authorization system, found the appropriate financial institution, and contacted that institution. It was time consuming and resource intensive. And it was not a temporary measure. Unless the coding enforcement program was maintained indefinitely, merchants would simply return to their

110 U.S. GEN. ACCOUNTING OFFICE, *supra* note 102, at 22.

111 *Id.* at 26.

112 *Id.*

113 *Id.* at 31–32. 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. VISA, *supra* note 21. In addition, Visa requires online gambling merchants to post certain notices: "a Website for an Online Gambling Merchant must contain . . . [t]he 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.' " *Id.* at 5.4.C.2.

114 U.S GEN. ACCOUNTING OFFICE, *supra* note 102, at 32.

115 *Id.*

116 *Id.*

117 *Id.*

118 *Id.*

119 *Id.*

previous practice of miscoding their transactions, thus undercutting the blocking scheme's effectiveness.

An additional way in which a payment system could react to the concern about internet gambling 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.[120]

The UIGEA required payment systems to have policies and procedures reasonably designed to stop illegal internet gambling transactions.[121] The implementing regulations required the affected parties to "establish and implement written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit" illegal internet gambling transactions.[122]

The statute creates a safe harbor for payment systems that adopt a coding and blocking scheme.[123] 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.[124] This description tracked the existing industry practices.

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. There are other ways to satisfy the general duty, but the presence of an approved safe harbor written into both the statute and the implementing regulations means that any replacement mechanism has to demonstrate that

---

120 *Id.* at 20–21.

121 Unlawful Internet Gambling Enforcement Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (codified at 31 U.S.C. §§ 5361–5367 (2006)).

122 12 C.F.R. § 233.5(a) (2009).

123 12 C.F.R. § 233.6(d)(1)(ii) (2009).

124 The code's relevant section reads:

> (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 . . . .

Id.

it is at least as effective as the approved safe harbor. The practical effect is to extend indefinitely the current coding and blocking system.

1. Implementation Challenges with the Internet Gambling Act

A key issue faced by payment intermediaries in implementing the new law was the need to clarify the status of certain gambling operations as legal or illegal. 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 regulations implementing the UIGEA generally define "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.[125]

However, the regulations "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."[126] The regulations "do[] not spell out which activities are legal and which are illegal, but rather relies on the underlying substantive Federal and State laws."[127]

The Federal Reserve Board and the Department of the Treasury (the Agencies) reasonably refused to try to define the unlawful internet gambling. Given the states' varying approaches to the regulation of gambling within their jurisdictions, it found that "the underlying patchwork legal framework does not lend itself to a single regulatory definition of 'unlawful Internet gambling.' "[128]

The difficulty of the issue can be seen in the context of horse racing. The existing statute appears to authorize internet betting on horse racing. The Interstate Horseracing Act (IHA) authorizes interstate off-track wagers and

---

[125] Prohibition on Funding of Unlawful Internet Gambling, 72 Fed. Reg. 56,680, 56,681 (Oct. 4, 2007) (to be codified at 12 C.F.R. § 233, 31 C.F.R. § 132).

[126] *Id.* at 56,681–82.

[127] *Id.* at 56,682.

[128] Prohibition on Funding of Unlawful Internet Gambling, 73 Fed. Reg. 69,382, 69,384 (Nov. 18, 2008) (to be codified at 12 C.F.R. pt. 233 & 31 C.F.R. pt. 132). For similar reasons, the Agencies declined to develop, publish and update a list of merchants who were in violation of the Act. *Id.*

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."[129]

The facial meaning of this definition seems to allow bets on horseracing to take place through electronic media, such as the Internet, provided that the transaction is 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 at the heart of a World Trade Organization (WTO) ruling finding that the IHA violated U.S. trade commitments.[130] 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.[131] The U.S. Department of Justice maintains that internet horse race betting is illegal.[132]

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.[133]

---

[129] Interstate Horseracing Act of 1978, 15 U.S.C. §§ 3001–3007 (2006). Interstate horseracing "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." *Id.* § 3002(3).

[130] Appellate Body Report, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 358–64, WT/DS285/AB/R (Apr. 7, 2005).

[131] *See* GOLDSMITH & WU, *supra* note 7, at 172–73 (discussing the WTO case).

[132] *See Internet Gambling Prohibition Act of 2006: Hearing on H.R. 4777 Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 109th Cong. 80 (2006) (testimony of Rep. John Conyers, Jr., Ranking Member, H. Comm. on the Judiciary) ("The Department of Justice views the existing criminal statutes as prohibiting the interstate transmission of bets or wagers including wagers on horse races." (quoting the Department of Justice's earlier statement)).

[133] 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." 31 U.S.C. § 5364(b)(4) (2006). 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 payment 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* Prohibition on Funding of Unlawful Internet Gambling, 73 Fed. Reg. 69,382, 69,391 (Nov. 18, 2008) (to be codified at 12 C.F.R. pt. 233 & 31 C.F.R. pt. 132).

This left the determination of the legality of horse betting to the payment systems. Card systems were permitted to continue using the industry gambling code as a way to implement the safe harbor, which could result in the blocking of some transactions that industry participants feel are perfectly legal.[134] 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.[135]

The legislation imposed indirect liability obligations on other parties in addition to financial institutions. The law allows the U.S. Attorney General (AG) or a state attorney general to ask a district court to enter a restraining order or injunction against any person in order to prevent or restrain an unlawful internet gambling transaction.[136] But these actions are limited in the case of interactive computer services.[137] Under this remedy, the AG can only ask the computer service to remove or disable access to a site, or link to a site, involved in illegal internet gambling, and it has to specifically identify the location of the offending site or link.[138] The request must be directed 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.[139] UIGEA reflects how pure internet intermediaries are treated differently from the traditional payment systems.

2. Internet Gambling Assessment

The experience of payment intermediaries in controlling illegal internet gambling can be assessed through the framework developed in Part II. This assessment consists of an equity analysis, a market analysis, and a cost-benefit analysis. The specific questions are: whether the online gambling legislation imposed an unfair burden (equity analysis); whether the market was adequately addressing the issue without it (market analysis); and whether it imposed burdens that exceeded their benefits and whether there was a feasible alternative that would achieve the same benefit at lower cost (cost-benefit analysis).

134 They were given liability protection for this possible over-blocking. *See id.*

135 *Id.* at 69,391–92.

136 31 U.S.C. § 5365(a)–(b) (2006).

137 *Id.* § 5365(c).

138 *Id.*

139 *Id.* An interactive computer service has the same meaning as in § 230 of the Communications Decency Act of 1996, *id.*, indicating that this provision has its roots in the same internet exceptionalist thinking that generated that statute.

On equity grounds, the payment system connection to internet gambling is too passive to justify imposing legal responsibility for blocking illegal internet gambling. Payment intermediaries are not to blame when others use their system for internet gambling because these intermediaries have no specific connection to the activity other than operating a general purpose payment system. They do not reap extra profits through special arrangements with the internet gambling merchants. Internet gambling transactions are no different from any other payment card transaction. On pure equity grounds alone, then, there is no reason to single out these transactions and impose special legal responsibilities.

A market analysis indicates that there are still some feasible enforcement arrangements that were not established prior to the passage of the internet gambling law. Although intermediaries may not be responsible for their customers' gambling, many of them are concerned about the social ills connected with the activity and want to reduce its prevalence.[140] U.S. financial intermediaries had already refused to sign up domestic internet merchants because these merchants were not authorized to act legally in the United States.[141] Some state attorneys general requested that the intermediaries block offshore gambling activities, and many cooperated.[142] These agreements did not extend to all financial institutions and did not cover all states, but they could have been extended without imposing a legislative requirement.

A cost-benefit analysis of UIGEA starts with an estimate of its effect on the amount of illegal internet gambling activity. 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.[143] A reduction in internet gambling activity in the United States resulted from the voluntary agreements just described. This reduction would continue after the legislation's compliance date. It is likely that the end result would be the substantial elimination of internet gambling by customers of U.S. financial institutions.

The costs associated with the payment systems' compliance with the legislation include the costs of maintaining and enforcing an internet gambling coding and blocking scheme, which is entirely manual and cannot

---

140 *See Financial Aspects of Internet Gaming Hearing*, *supra* note 103, at 25–26 (statement of Mark MacCarthy, Senior Vice President, Public Policy, Visa U.S.A., Inc.).

141 *Id.* at 26; U.S. GEN. ACCOUNTING OFFICE, *supra* note 102, at 20.

142 *See, e.g.*, GOLDSMITH & WU, *supra* note 7, at 82 (discussing Spitzer's efforts "to convince every major American credit card provider and online payment system to stop honoring web gambling transactions").

143 Eric Pfanner & Heather Timmons, *U.K. Seeks Global Rules for Online Gambling*, INT'L HERALD TRIB., Nov. 2, 2006, at 14.

be automated. This Section highlights the additional costs associated with increases in international tensions, the copycat effect, and over-blocking.

There are substantial costs associated with increased tension in international relations. The United States' passage of the internet gambling law was one of the first unilateral legislative actions by a major jurisdiction using intermediaries to enforce local law on the Internet. It had substantial international relations repercussions. Reactions to the U.S. internet gambling legislation from abroad have not been favorable. 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."[144] While Britain was seeking to develop a consensus on a global standard for legalizing and regulating internet gambling,[145] the U.S. law went in the opposite direction of taking unilateral action to close off the U.S. market.

The WTO reaction, concerning the legality of the United State's action in light of its trade commitments, continues to stir international trade and political issues.[146] Among the costs of using intermediaries to bar internet gambling transactions are these continuing conflicts. For example, in June 2009, the European Union released a report criticizing the U.S. internet gambling laws, asserting that they violated WTO agreements, and urging negotiation to resolve the issues.[147]

International concerns about the U.S. gambling law may also prompt costs stemming from the copycat effect, which uses the assignment of 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 as one of the costs of the legislation deserving consideration.

Judge Kozinski, dissenting in *Perfect 10*, demonstrates 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."[148] Simply put, the argument is that since payment system contracts bar all illegal activity, 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

144 *Id.* (quoting Tessa Jowell).

145 *Id.*

146 *See supra* note 130 and accompanying text.

147 Press Release, European Comm'n, EU Commission Publishes Report on US Internet Gambling Laws (June 10, 2009), *available at* http://europa.eu/rapid/press ReleasesAction.do?reference=IP/09/902.

148 Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 824 (9th Cir. 2007) (Kozinski, J., dissenting) (internal citations omitted).

gambling, why not elsewhere?" Indeed, why not everywhere? And once the precedent is set, it is hard to return to a detailed analysis of the facts to see if indirect liability makes sense in a specific case.

The copycat effect could very well extend globally. First, it might encourage other countries to use payment systems to implement their own internet gambling regimes. The copycat effect easily extends to other areas of law. It is worth considering how a French court approaching the Yahoo! case and influenced by the copycat effect might exert authority over French financial institutions. In this case, a French court attempted to require Yahoo!, a U.S. company, to prevent the online sale of Nazi paraphernalia to French citizens, which was prohibited under French law.[149] The new U.S. internet gambling law reveals an additional strategy that could be made available to French enforcement entities: deputizing 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 by establishing reasonable policies and procedures that prevent the use of the French banking facilities for payment of transactions involving Nazi paraphernalia.

Such an application of U.S. gambling law would have extremely costly results, not just for the international payment brands but for all financial institutions globally. To avoid this obligation, French financial institutions would have to drop out of global payment networks, something they would be reluctant to do. If they chose to remain part of the global payment system, the global payment system would have to modify itself in order to accommodate this new obligation. For example, a coding and blocking scheme would no longer be feasible because the content of retail transactions is not coded in payment system transaction messages. Furthermore, a code for Nazi paraphernalia would be much too specific for any business needs. To implement the rule, the global payment systems would have to require that all banks in their system ensure that their merchants do not submit

---

[149] *L'Union des Etudiants Juifs de France (UEJF), la Ligue Contre le Racisme et L'Antisemitisme (LICRA) v. Yahoo!, Inc. et Yahoo France* , T.G.I. Paris, Nov. 20, 2000, (Reporter) 05308, Gaz. Pal. 2000, somm. jurispr. 1307. The ultimate French enforcement power was over assets that Yahoo! had in France. *Id.* Yahoo! could have avoided this enforcement power by simply withdrawing from France. 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. Similar issues arise in conjunction with a suit against Wikipedia by a convicted murderer who is invoking Germany's privacy laws in a bid to remove references to his killing of a Bavarian actor in 1990. *See* David Kravets, *Convicted Murderer Sues Wikipedia, Demands Removal of His Name*, WIRED, Nov. 11, 2009, http://www.wired.com/ threatlevel/2009/11/ wikipedia_murder/#ixzz0el12tNDD.

transactions involving Nazi paraphernalia and customers of French banks. Enforcing this effectively would require locating the internet sites involved in these sales, perhaps through their advertisements or through searching the web for appropriate keywords and symbols. Further steps might involve doing test transactions using a card issued by a French bank, and then taking enforcement steps against merchants submitting transactions for authorization in violation of this rule.

Another cost, as introduced above, is the over-blocking problem created by the way in which payment intermediaries comply with UIGEA. Perfectly legal transactions will likely be blocked because payment intermediaries cannot distinguish them from illegal transactions. This example illustrates that intermediaries are usually better than others at monitoring their own systems for business activity of a certain type, but not at detecting the illegality of activity on their systems.[150] The point arises in internet gambling because the codes used by financial institutions reflect the business activity of gambling, not its status as legal or illegal. As a result, the payment systems' policies and procedures, which were adopted to comply with the Act and which have been accepted by the implementing regulations, over block and prevent perfectly legal activity from taking place.[151]

---

[150] *See* Mann & Belzley, *supra* note 8, at 278 ("Surely eBay is more adept at searching and monitoring its marketplace than Tiffany & Co., while eBay probably is not as effective as Tiffany & Co. in distinguishing bona fide Tiffany products from counterfeits."); *see also* Schruers, *supra* note 68, at 252 ("[T]he 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."). Schruers adds that in this case, the wronged party may be better suited to the task of locating the offending content. *Id.* at 252.

[151] Mann & Belzley, *supra* note 8, at 294. Mann and Belzley present a useful discussion of this over-blocking issue:

> [A] risk always exists that imposing additional burdens on intermediaries will chill the provision of valuable goods and services. That will be especially problematic in cases where considerable risk of chilling legal conduct that is adjacent to the targeted conduct exists. As discussed below, that might tend to make the use of intermediaries less plausible in file-sharing contexts where determining whether any particular act of file-sharing is illegal is difficult, and much more plausible in the gambling context where in many cases substantially all traffic to a particular site likely involves illegal conduct. Requiring intermediaries to make those kind 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.

Id. at 274. The internet gambling case illustrates that determining when a website is engaged in illegal gambling is not a simple task. It is fraught with the kind of "subjective decisions" that Mann and Belzley are properly concerned about. Payment systems faced with this difficulty do not to make these subjective decisions, but block all gambling activity, including legal gambling transactions.

In light of this difficulty, there might be more effective ways of assigning liability. The new law creates unnecessary confusion by failing to define the term "unlawful internet gambling." As Congressman Barney Frank wrote to former Secretary of the Treasury Henry 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."[152] He has introduced legislation to regulate internet gambling merchants.[153] It would require the Secretary of the Treasury to license internet gambling establishments, and would provide immunity for financial service companies who process transactions to licensed entities.[154] The licensing process would be the exclusive way for internet gambling sites to operate legally.[155] The obligations to block transactions from other, unlicensed internet gambling merchants would remain.[156] The lack of clarity about which merchants are legal would be resolved through the licensing process. At best, the system would rely on a list of approved gambling entities that the payment networks could check before approving gambling transactions from particular internet merchants.

To be effective, however, this list would have to be coordinated with other jurisdictions. Payment systems might respond to such a 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

---

[152] Press Release, House Comm. on Fin. Servs., Frank Calls on Bush Administration to Delay Internet Gambling Regulations (Nov. 10, 2008), *available at* http://www.house.gov/apps/list/press/financialsvcs_dem/11102008.shtml. Chairman Frank wrote that he "introduced legislation (HR 5767, later HR 6870) that would prohibit the implementation of these flawed rules and replace them with a formal rulemaking process that would define the term 'unlawful internet gambling,' something the proposed rules fail to do." *Id.* House Bill 6870 was passed by the Financial Services Committee on September 16, 2008. *Id.* But the Agencies issued their final rules in November 2008. Press Release, Bd. of Governors of the Fed. Reserve Sys., Agencies Issue Final Rule to Implement Unlawful Internet Gambling Enforcement Act (Nov. 12, 2008), *available at* http://www.federalreserve.gov/newsevents/press/bcreg/20081112b.htm. In November 2009, the compliance date for the internet gambling rules was postponed for six months. *See* Press Release, Bd. of Governors of the Fed. Reserve Sys., Agencies Extend Compliance Date for Final Rule to Implement Unlawful Internet Gambling Enforcement Act (Nov. 27, 2009), *available at* http://www.federalreserve.gov/newsevents/press/bcreg/20091127a.htm [hereinafter Press Release, Agencies Extend Compliance Date for Final Rule].

[153] Internet Gambling Regulation, Consumer Protection, and Enforcement Act, H.R. 2267, 111th Cong. (2009).

[154] *Id.* §§ 5383, 5385.

[155] *Id.* § 5383.

[156] *See id.* § 5385 (implying blocking by implication).

United States 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. Secretary of the Treasury might not be authorized by other countries. These other countries could seek to enforce Congressman Frank's proposed law by limiting the ability of their banks to accept any internet gambling transactions. Moreover, other countries might have their own legal requirements for registering and regulating internet gambling establishments. 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. 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 for a few countries in the short term could easily collapse if each country attempts to use it for the purpose of enforcing local rules.

None of these issues are imminent, however, and the new licensing regime proposed in Congressman Frank's legislation would be an improvement over the existing system in the short term. But over time the only way payment systems can operate is through a reduction in the diversity of the laws they must accommodate. This suggests that the government either seeks other ways to enforce its local laws or begins the process of harmonizing its laws. In the case of internet gambling, one solution would be an international agreement recognizing licensing arrangements in different countries as long as they satisfy certain agreed upon minimum standards.[157]

B. CHILD PORNOGRAPHY, CONTROLLED SUBSTANCES, AND ONLINE TOBACCO

1. Child Pornography[158]

Payment intermediaries and most other internet intermediaries have explicit policies against child pornography.[159] This section examines more

---

[157] The postponed compliance date, Press Release, Agencies Extend Compliance Date for Final Rule, *supra* note 152, might provide time for such an agreement to be drafted and adopted.

[158] Portions of this Section are taken directly from the author's congressional testimony, as cited.

[159] Google bans child pornography. Making the Internet Safe for Kids: The Role of ISP's and Social Networking Sites: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce, 109th Cong. 137 (2006) (testimony of Nicole Wong, Associate General Counsel and Chief Privacy Officer, Google Inc.). Nicole Wong stated,

> As a company, Google is deeply committed to protecting children on the Internet in our actions and in our guiding principles. Child pornography is a horrific and vicious crime and has no place in a civilized society. Google has a zero-tolerance policy for child pornography and those who would

specifically how payment intermediaries take steps to prevent commercial child pornography transactions.[160]

Card payment systems work closely with law enforcement to remove any merchants in their systems that are involved in child pornography. In addition, they actively screen merchants for this illegal activity without a legal compulsion to do so and without waiting for complaints from law enforcement or other third parties.[161]

Specifically, card payment systems enforce their prohibition against child pornography with a two-part program.[162] The first part is a set of due diligence requirements designed to prevent child pornography merchants from entering payment systems. The second part is a monitoring program to detect and expel any child pornography merchants that manage to fraudulently enter the systems.[163]

> promote it. When we become aware of child pornography anywhere in our search 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 to help track down online criminals and child predators.

Id. Visa explicitly bans child pornography from its payment system, stating in its International Operating Regulations,

> 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 [t]erminate 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, *supra* note 21, at 4.1.C.5.b (emphasis in original). MasterCard also bans child pornography as its general rule against illegal transactions applies to "[t]he 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, *supra* note 21, at 5.9.7.

160 This account of Visa's policies and procedures on child pornography is based on my Congressional testimony. *Deleting Commercial Pornography Sites from the Internet: The U.S. Financial Industry's Efforts to Combat This Problem: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. 70–72 (2006) [hereinafter *Deleting Commercial Pornography Sites From the Internet Hearing*] (statement and testimony of Mark MacCarthy, Senior Vice President, Public Policy, Visa, U.S.A., Inc.). American Express, MasterCard, and PayPal have similar policies and procedures. *See id.* at 51–58 (statement of Arne L. Christenson, Senior Vice President, Federal Governmental Affairs, American Express Company); *id.* at 60–63 (statement of Jodi Golinsky, Vice President & Senior Regulatory Counsel, MasterCard International, Inc.); *id.* at 66–67 (statement of Joe Sullivan, Associate General Counsel, PayPal, Inc.).

161 *Id.* at 71 (statement and testimony of Mark MacCarthy, Senior Vice President, Public Policy, Visa, U.S.A., Inc.).

162 *Id.* at 70.

163 *Id.* at 71.

The card systems require financial institutions that are part of their payment network to ensure that all merchants are properly qualified to accept payment cards.[164] This normally involves a determination that a prospective merchant is financially responsible, and will abide by system requirements and applicable law.[165]

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 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.[166]

Accordingly, the payment systems supplement these due diligence requirements with an active monitoring system. Traditional payment networks maintain separate monitoring campaigns to identify and eliminate transactions from child pornography merchants. Visa's program, for example, began in 2002.[167] Visa 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 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 webpages each month.[168]

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 pertaining to child pornography. This creates the possibility, to be discussed later, of achieving greater efficiency by having a common search program rather than duplicative individual detection efforts.

---

164 *Id.*

165 There are a variety of methods that financial institutions may use to determine these qualifications, such as reviewing credit reports, business financial statements, and income tax returns, conducting physical inspections of the business premises of prospective brick and mortar merchants, and obtaining a detailed business description of electronic commerce merchants and examining merchants' websites. *Id.*

166 *Id.*

167 *Id.*

168 *Id.* at 72.

The payment systems do the monitoring themselves because it helps them take the next step: determining which of the apparently active child pornography websites actually accept the cards for transactions. When the outside search firm detects one of these problematic sites, it conducts test transactions to see whether the site is actually accepting the brand's cards or whether they are merely using the trademark illegally on their site. The search firm tells the card network immediately if it finds a site that is accepting the network's cards for these transactions. Unless requested by law enforcement to leave these sites open,[169] the network then contacts any financial institution found to be processing these child pornography transactions and directs it to stop processing these transactions immediately. If the financial institutions have not done so within seven calendar days, they are fined.[170]

If these identified sites are not actually accepting the payment cards, but are merely using the trademarks on their site, the networks use their best efforts to locate the web hosting companies to direct them to remove the logo.[171] In addition, the payment networks, such as Visa, provide information regarding all these sites to U.S. and international law enforcement officials.

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.[172] In March 2006, payment systems and financial institutions joined with the NCMEC to form the Financial Coalition Against Child Pornography and announced the formation of this group at a press conference attended by Senator Shelby.[173] The group shares information and takes collective action against child pornography merchants identified by complaints to the NCMEC hotline or from internet searches. This effort has produced some positive results in disrupting the activities of child pornographers and pushing bad actors away

169 If requested, the networks do allow problematic sites to remain operational as part of an ongoing law enforcement investigation. *Id.*

170 *Id.*

171 *Id.*

172 *Combating Child Pornography by Eliminating Pornographers' Access to the Financial Payment System: Hearing Before S. Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. 51 (2006) [hereinafter *Combating Child Pornography Hearing*] (statement of Ernie Allen, President and Chief Executive Officer, National Center for Missing & Exploited Children).

173 *Id.* at 97 (statement of Mark MacCarthy, Senior Vice President, Public Policy, Visa USA, Inc.).

from recognized payment brands and toward less traditional payment mechanisms.[174]

The effectiveness of the payment card campaign is reflected in industry statistics. For instance, in August 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.[175] Since the beginning of 2006, nine such sites had been identified.[176] All of these sites were quickly expelled from the Visa system.[177]

In summary, the process developed by the payment systems to control child pornography transactions consists of pro-active monitoring followed by aggressive efforts to expel child porn merchants from the system. No legal compulsion exists to take this action, but it is done in close cooperation with law enforcement and other private bodies.

2. Controlled Substances[178]

Internet intermediaries also take extra precautions to protect against the use of their systems for traffic of controlled substances.[179] Payment systems treat controlled substances similar to 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 systems, while allowing legitimate internet pharmacies to function normally.[180]

---

174 *See Deleting Commercial Pornography Sites From the Internet Hearing*, *supra* note 160, at 30 (statement of Ernie Allen, President and Chief Executive Officer, National Center for Missing & Exploited Children) ("We are seeing indications of a trend toward directing buyers away from credit cards and toward alternative payment methods to make the actual transaction."). Allen also stated that "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." *Id.* at 27.

175 *Id.* at 69 (testimony of Mark MacCarthy, Senior Vice President, Public Policy, VISA U.S.A., Inc.).

176 *Id.*

177 *Id.*

178 Portions of this Section are taken directly from the author's congressional testimony, as cited.

179 For example, Microsoft, Yahoo!, and Google all require U.S. based pharmaceutical advertisers to be registered with PharmacyChecker. PharmacyChecker.com Verification Program, https://www.pharmacychecker.com/sealprogram/choose.asp (last visited Feb. 4, 2010) ("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.").

180 This summary of the policies and procedures used to combat controlled substances

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.[181] In 2004 and 2005, payment system representatives met with the Food and Drug Administration (FDA) and the Drug Enforcement Administration (DEA) to develop strategies to deal with the problem of controlled substances sales on the Internet.[182] 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.[183]

Coding the nature of the transaction so that financial institutions could block as necessary, which is effective for gambling transactions, does not work in the instance of controlled substances. Available codes can only identify the business of the website, not the nature of the pharmaceuticals dispensed. Many legitimate websites sell pharmaceuticals under appropriate government regulation and private sector oversight. If the business code were used as a trigger to block these transactions, it would eliminate a substantial and desirable internet business as well.

The only effective approach is 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 responsibility to ensure that only legal transactions enter the Visa Payment System and directed the affiliates' attention to the lists of controlled substances and problematic drugs on the FDA and DEA websites.[184] Visa also directed its members to the public safety bulletins on the FDA website about buying medicines online.[185] Visa 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

---

is based on my congressional testimony. *Safety of Imported Pharmaceuticals: Strengthening Efforts to Combat the Sales of Controlled Substances over the Internet: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce*, 109th Cong. 174–76 (2005) [hereinafter *Safety of Imported Pharmaceuticals Hearing*] (statement of Mark MacCarthy, Senior Vice President, Public Policy, VISA, U.S.A., Inc.). MasterCard has a similar program in place. *Id.* at 178–81 (statement of Michael McEneney, Partner, Sidley, Austin, Brown, & Wood, LLP).

[181] *Id.* at 174 (statement of Mark MacCarthy, Senior Vice President, Public Policy, VISA, U.S.A., Inc.).

[182] *Id.*

[183] *Id.* at 214–15 (testimony of Andrew McLaughlin, Senior Policy Counsel, Google, Inc.).

[184] *Id.* at 175 (statement of Mark MacCarthy, Senior Vice President, Public Policy, VISA, U.S.A., Inc.).

[185] *Id.*

licensed in the United States to write prescriptions, and provide a way to speak to a person about problems.[186] Visa also advised its members to consider relying on a reputable seal program, such as the Verified Internet Pharmacy Practices Site Program operated by the National Association of Boards of Pharmacy, as a means of identifying reputable internet pharmacies.[187] 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.[188]

As in the case of child pornography, these due diligence efforts are necessary but not sufficient. The payment networks each retain the services of an outside firm to search the Internet for websites selling controlled substances and accepting the networks' payment cards.[189] This program builds on the efforts to monitor the Internet for child pornography, using the same web crawling and filtering technology and the same outside search firm to conduct sweeps. This vendor looks for websites that display the card's brand 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 webpages each month. The networks then take steps to remove merchants who appear to be selling controlled substances.[190]

These efforts have produced positive results. In 2005, MasterCard indicated that they had located and shut down 500 websites selling illegal controlled substances.[191] 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 in the availability of controlled substances.[192] In 2008, however, it documented a decline in the number of websites advertising or

186 *Id.*

187 *Id.*

188 *Id.*

189 *Id.*

190 *Id.*

191 Visa's program shut down 49 similar sites. For statistics from both payment networks, see *id.* at 208 (testimony of Mark MacCarthy, Senior Vice President, Public Policy, VISA, U.S.A., Inc.).

192 *See Rogue Online Pharmacies: The Growing Problem of Internet Drug Trafficking: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 7–9 (2007) [hereinafter *Rogue Online Pharmacies Hearing*] (statement of Joseph A. Califano, Jr., Chairman and President, The National Center on Addiction and Substance Abuse at Columbia University) (summarizing the early studies' findings that "[o]ver the 4-year course of our analysis, the number of selling sites has climbed from 154 [in 2004 and 2005] to 187 [in 2007]").

selling controlled substances, and suggested that this decline could be attributed to financial service company efforts to block controlled substance transactions.[193]

3. 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.[194]

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.[195] 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

[193] Press Release, Nat'l Ctr. on Addiction & Substance Abuse at Columbia Univ., New CASA Report Finds: Most Web Sites Selling Prescription Opioids, Stimulants and Depressants Require No Prescription; Some Sites Now Sell Prescriptions and Online "Medical Consultations" to Get Controlled Drugs 1 (July 9, 2008), *available at* http://www.casacolumbia.org/absolutenm/templates/PressReleases.aspx?articleid=531&zoneid=66 ("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."). 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." *Id.* (quoting Joseph A. Califano, Jr., CASA's Chairman and President). The large number of websites 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 forty-five 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. NAT'L CTR. ON ADDICTION AND SUBSTANCE ABUSE AT COLUMBIA UNIV., "YOU'VE GOT DRUGS!" V: PRESCRIPTION DRUG PUSHERS ON THE INTERNET 13 (2008), *available at* http://www.casacolumbia.org/articlefiles/531-2008%20You%27ve%20Got%20Drugs%20V.pdf. Test transactions by the payment systems revealed that only four of these sites actually attempted to process a transaction. *Id.* 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." *Id.*

[194] For instance, Google does not accept online advertisements for tobacco products. *See* Google AdWords, Advertising Policies: Tobacco and Cigarettes, http://adwords.google.com/support/aw/bin/static.py?page=guidelines.cs&topic=all&answer=47228&country=US&adtype=text (last visited Mar. 25, 2010) ("Advertising is not permitted for the promotion of tobacco or tobacco-related products, including cigarettes, cigars, tobacco pipes, rolling papers, electronic cigarettes, and e-cartridge cigarettes.").

[195] Consumeraffairs.com, Credit Card Companies Snuff Online Tobacco Sales (Mar. 17, 2005), http://www.consumeraffairs.com/news04/2005/tobacco_ags.html.

brought to the attention of the intermediaries, they would respond by taking voluntary measures to stop the illegal transactions. Because 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.[196]

In January 2005, forty-two state attorneys general wrote to the payment card networks informing them that virtually all online tobacco retailers engage in illegal sales.[197] They listed the laws they believed were violated and requested that the payment networks not allow their cards to be used for online tobacco product purchases until retailers proved that their sales were not in violation of state or federal laws.[198] 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.[199]

In March 2005, after several joint meetings, the card companies reached an agreement with the state attorneys general and with BATF to take steps against the online sale of tobacco products, including adopting policies prohibiting use of their cards for the illegal online sale of cigarettes and taking action against any such sellers identified by law enforcement.[200]

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 were in compliance with relevant laws.[201] Unlike the case of child pornography and

---

196 *Id.*

197 *Id.*

198 *Id.*

199 *Id.*

200 There was only a release; the agreement itself was verbal. Press Release, Office of the Att'y Gen., State of N.Y., State AGs and ATF Announce Initiative with Credit Card Companies to Prevent Illegal Internet Cigarette Sales (Mar. 17, 2005), *available at* http://www.ag.ny.gov/media_center/2005/mar/mar17b_05.html. The release announcing 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.

Id.

201 *MasterCard Urges Merchant Compliance with Rules Governing the Internet Sale of Tobacco*, BUS. WIRE, Mar. 8, 2005, *available at* WestLaw, 3/8/05 BWIRE 15:00:00 ("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

controlled substances, however, the payment networks relied on complaints from law enforcement, instead of conducting their own investigations, to direct their efforts to stop the illegal activity. As a result of these steps, the number of online tobacco merchants declined dramatically. MasterCard estimated that they had cut off the 100 largest online sites.[202]

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 to stop delivering cigarettes for illegal internet sellers.[203] In October 2005, UPS agreed to stop shipping cigarettes to consumers throughout the United States.[204] In February 2006, FedEx agreed to stop shipping cigarettes from online stores.[205] The U.S. Postal Service rejected the request to stop delivering cigarettes from online tobacco stores, citing federal requirements that it deliver the mail.

4. *Assessment of Child Pornography, Controlled Substances, and Online Tobacco*

Child pornography, controlled substances, and online tobacco can be discussed together because they raise common issues. They all involve extensive cooperation between payment systems and federal government agencies policing criminal activity on the Internet. As discussed in the previous sections, payment networks monitor their systems for transactions involving child pornography and controlled substances, and share the results with law enforcement. In the case of online tobacco, they react to complaints brought to them by law enforcement. These enforcement arrangements emerged in the absence of any legal compulsion.

The assessment of public policies in this area follows the framework outlined in Part II. The analysis of equities suggests that payment

---

any applicable State Attorney General.").

[202] Bob Tedeschi, *E-Commerce Report; Now that Credit Card Companies Won't Handle Online Tobacco Sales, Many Merchants Are Calling It Quits*, N.Y. TIMES, Apr. 4, 2005, at C5; GOLDSMITH & WU, *supra* note 7, at 76–77; Mann & Belzley, *supra* note 8, at 247; *see also* COMM. ON REDUCING TOBACCO USE: STRATEGIES, BARRIERS & CONSEQUENCES, INST. OF MED. OF THE NAT'L ACADS., ENDING THE TOBACCO PROBLEM: A BLUEPRINT FOR THE NATION 670 (Richard J. Bonnie et al. eds., 2007), *available at* http://www.nap.edu/openbook.php?isbn=0309103827.

[203] Press Release, Office of the Att'y Gen., State of N.Y., Leading Package Delivery Company Agrees to Stop Shipping Cigarettes to Individual Consumers (July 5, 2005), *available at* http://www.ag.ny.gov/media_center/2005/jul/jul05a_05.html.

[204] Press Release, Office of the Att'y Gen., State of N.Y., UPS Joins Effort to Reduce Youth Smoking (Oct. 24, 2005), *available at* http://www.ag.ny.gov/media_center/2005/oct/oct24a_05.html.

[205] Press Release, Office of the Att'y Gen., State of N.Y., FedEx to Strengthen Policies Restricting Cigarette Shipments (Feb. 7, 2006), *available at* http://www.ag.ny.gov/media_center/2006/feb/feb07a_06.html.

intermediaries have a general responsibility to take affirmative action in this area, but the market analysis suggests that they are already living up to these responsibilities. There is no need for legal compulsion. The costs of additional legal burdens are likely to be higher than any benefits from the increase in their efforts to control these illegal activities.

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 would not have affirmative responsibilities 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 controlled substances sales is substantial.[206] While this is undoubtedly a normative view, it is one that is widely, if not universally, shared. As a result, payment systems should take positive steps in this area to prevent the use of their systems for these purposes. System monitoring is needed because it is the most effective way to catch these bad actors if they manage to slip into the system.

Because of the public health issues involved, payment systems also owe a duty to respond in the area of online tobacco sales. In this case, however, the payment networks have calibrated their response to the needs of law enforcement. Law enforcement is able to efficiently investigate cases and bring them to the attention of the payment systems. Responsiveness to these complaints, rather than pro-active system monitoring, is acceptable.

Intermediaries are cooperating fully with the relevant government agencies to satisfy these general obligations. As discussed above, the steps that the payment card industry has taken to cooperate with law enforcement have successfully controlled commercial online child pornography, illegal sales of controlled substances, and online tobacco sales. There is no need for additional regulatory requirements.[207]

---

[206] For harms caused by the internet sales of controlled substances, see *Rogue Online Pharmacies Hearing*, *supra* note 192, at 10–11 (statement of Philip B. Heymann, James Barr Ames Professor of Law, Harvard Law School). For the extent of child pornography, see *Combating Child Pornography Hearing*, *supra* note 172, at 25–26 (testimony of Ernie Allen, President and Chief Executive Officer, National Center for Missing and Exploited Children). *See also* National Center for Missing and Exploited Children, What is Child Pornography?, *available at* http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=1504 (last visited Mar. 5, 2010).

[207] Mann and Belzley note that

> regulators in a variety of contexts have reached informal agreements with intermediaries in which intermediaries voluntarily agree to cooperate. Most of those agreements seemingly do not reflect the view of the intermediaries that they could be forced in litigation to provide that

Despite the success of these voluntary efforts, Congress has proposed legal requirements on payment systems to control child pornography and controlled substances. Proposed legislation mandates further efforts by intermediaries to prevent the use of their systems for child pornography.[208] 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 . . . ."[209] 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."[210] The Bill also imposes a two year record keeping requirement on ISPs and others to facilitate child pornography investigations.[211] In light of the extensive efforts already undertaken by intermediaries in this area, it is unlikely that these requirements will produce any additional net benefit.

Congress passed legislation regulating online pharmacies in 2008.[212] This law imposes obligations on U.S. based internet pharmacies regarding controlled substances and prohibits the sale of controlled substances except as specifically authorized.[213] The law requires that certain intermediaries must not "knowingly or intentionally . . . aid or abet" any unauthorized sale of controlled substances.[214] The statute defines 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]

> 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.

Mann & Belzley, *supra* note 8, at 260 n.59. But if the pressure to cooperate "in the shadow of potential law" has worked, why actually legislate?

208 Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009, H.R. 1076, 111th Cong. (2009).

209 *Id.* § 2.

210 *Id.* § 3. The Center for Democracy and Technology (CDT) 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." Memorandum from John Morris & Gregory T. Nojeim, Ctr. for Democracy & Tech. to Interested Persons 1 (June 18, 2009) (on file with author) (emphasis in original).

211 *See* H.R. 1076, § 5. CDT's analysis of this provision notes the difficulties record retention would create for ISPs and the tension with privacy concerns. Memorandum from John Morris & Gregory T. Nojeim, *supra* note 210, at 2–3.

212 Ryan Haight Online Pharmacy Consumer Protection Act of 2008, Pub. L. No. 110-425, 122 Stat. 4820 (codified in 21 U.S.C. §§ 829, 802).

213 *Id.* § 3(f)(1)(A).

214 *Id.* § 3(f)(1)(B).

dispensing of a controlled substance . . . ."[215] It is not clear that these requirements apply to payment systems.[216] Nonetheless, it is very likely that current financial intermediary processes would easily satisfy these general requirements if they applied.

As in the case of internet gambling, the new online pharmacy bill carried over the exemptions from liability first developed in § 230 of the Communications Decency Act for pure internet intermediaries.[217] 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.[218]

This exemption from liability appears justified for these parties because they are far removed from the actual causation of the illicit transactions, their involvement is passive, and they undertake substantial efforts to control the sale of controlled substances online. This exemption should also be extended to payment systems, given their substantial role in fighting these illegal activities in conjunction with law enforcement.

On cost grounds, however, the current arrangements could be improved. Payment systems have no particular expertise in monitoring their own systems for child pornography and controlled substances. The networks have outsourced their system monitoring efforts, and some efficiency could be achieved by combining these efforts, in coordination with appropriate law enforcement.[219]

---

[215] *Id.* § 3(f)(2)(C).

[216] *See* Sarah Rubenstein, *New Bill Targets Rogue Druggists on the Internet*, WALL ST. J., Oct. 9, 2008, at D1 ("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.").

[217] Ryan Haight Online Pharmacy Consumer Protection Act of 2008, Pub. L. No. 110-425, § 3(f)(3)(A)(iii), 122 Stat. 4820 (codified in 21 U.S.C. §§ 829, 802).

[218] *Id.* § 3(f)(3)(A)(iii).

[219] 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. *See, e.g.*, *Rogue Online Pharmacies Hearing*, *supra* note 192, at 11 (statement of Philip B. Heymann, James Barr Ames Professor of Law, Harvard Law School). 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. *Id.* 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

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.[220] This improvement, however, would require substantial international coordination to be effective.

C. ONLINE COPYRIGHT INFRINGEMENT

When payment intermediaries take steps against internet gambling merchants, child pornographers, purveyors of controlled substances, and online tobacco merchants, they are acting together with law enforcement officials. The information they gather in the searches of their systems are provided to law enforcement, and they react to complaints brought to them by law enforcement agencies. In contrast, with copyright cases, the complaining party is a private party alleging that some other party has harmed them by infringing on their copyright.

On its face, this is a very awkward place for intermediaries to be. In copyright infringement cases, private parties dispute their respective rights under the law. No adjudication has been made on the merits of the case. In some instances, no legal assertion of rights is 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? The third party may not know who is right. And if it does take action, but chooses the wrong side, the aggrieved party may pursue the third party for taking wrongful action.

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. The result is well-developed notions of secondary liability for copyright infringement that involve intermediaries.[221] These doctrines of secondary liability have evolved substantially over the past decades.

1. Legal Context for Intermediary Liability in Copyright Infringement

Court cases and federal statute define some indirect responsibilities of intermediaries regarding copyright. The 1984 Supreme Court decision in *Sony Corp. of America v. Universal City Studios, Inc.*[222] established a standard for assessing third party liability. Providers of a technology that can be used for

enforcement, however, would create some savings.

[220] *See Safety of Imported Pharmaceuticals Hearing*, supra note 180, at 206 (statement of Michael McEneney, Partner, Sidley, Austin, Brown, & Wood, LLP).

[221] For a brief discussion of vicarious and contributory liability in copyright law, see Lichtman & Landes, *supra* note 39.

[222] 464 U.S. 417 (1984).

infringing activities are not liable when there are "substantial non-infringing uses" of the technology.[223] The DMCA enabled copyright owners to enforce their existing rights in the Internet context by enlisting the help of internet intermediaries.[224] The key mechanism for gaining the cooperation of intermediaries is a safe harbor from secondary liability. ISPs are given an exemption from secondary liability so long as they act as a pure conduit, providing only transitory communications and system caching.[225] Web hosts and search engines also receive a safe harbor, provided they comply with a specific notice-and-takedown procedure.[226] Upon receiving notification of claimed infringement, the provider must expeditiously take down or block access to the material.[227]

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 where the third party is affirmatively involved in fostering the infringement. In an early file-sharing case, the Ninth Circuit found that the peer-to-peer service Napster was liable for secondary infringement based on its control and facilitation of its users' infringement of music copyrights.[228] The company subsequently went out of business in its original form.[229] More recently, the Supreme Court found that another peer-to-peer service, Grokster, violated federal copyright law when it took "affirmative steps . . . to foster infringement . . . by third parties," such as advertising an infringing use or instructing how to engage in an infringing use.[230]

Against this background arose a question regarding payment systems: are they liable for secondary infringement when their payment systems are used for direct infringement? In *Perfect 10 v. Visa International Service Ass'n*,[231] a

---

223 *Id.* at 442.

224 17 U.S.C. § 512 (2006).

225 17 U.S.C. § 512(a).

226 17 U.S.C. § 512(b).

227 *Id.*

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

229 Benny Evangelista, *Napster Runs Out of Lives—Judge Rules Against Sale*, S.F. CHRONICLE, Sept. 4, 2002, at B1.

230 MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 919 (2005).

231 494 F.3d 788 (9th Cir. 2007); *see* Jonathan Band, *The Perfect 10 Trilogy*, 5 COMPUTER L. REV. INT'L 142 (2007) (discussing *Perfect 10 v. Visa International Service Ass'n* and its relationship to similar secondary liability cases). Band summarizes the Visa case:

> 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.

Id. at 5. Judge Kozinski's dissent is indeed stinging, but it also underestimates the burden

subscription adult-content website alleged that numerous websites based in several countries had stolen its proprietary images, altered them, and illegally offered them for sale online.[232] Visa did not deny payment services to the allegedly infringing sites in response to the complaints, and Perfect 10 brought a contributory and vicarious infringement action against Visa.[233] The Ninth Circuit affirmed the district court to reject liability for Visa.[234]

In *Perfect 10*, the Ninth Circuit dismissed the charge of contributory infringement by focusing on whether the card companies "materially contributed" to the infringement.[235] The court said the credit card companies did not materially contribute to the infringement because they had no "direct connection" to the infringement.[236] 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.[237] 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 making a material contribution.[238]

The court made a similar point about vicarious liability, finding that the card companies had no practical ability or right to prevent the infringing activity.[239] While credit card services can exert financial pressure on the infringing websites, they cannot stop the actual reproduction or distribution of the infringing images.[240]

In his dissent, Judge Kozinski rejected both arguments.[241] According to Judge Kozinski, the card companies were directly connected to the infringement because they provided payment services.[242] Without these payment services there would be no infringement.[243] The card companies had the contractual right to terminate illegal activity on their systems, as well as the practical ability to exert financial pressure to stop or limit the infringing activity.[244]

---

that secondary liability would place on intermediaries. *Id.*

232 *Perfect 10*, 494 F.3d at 793.

233 *Id.*

234 *Id.*

235 *Id.* at 796.

236 *Id.*

237 *Id.*

238 *Id.* at 797.

239 *Id.* at 803.

240 *Id.* at 804.

241 *Id.* at 810–11 (Kozinski, J., dissenting).

242 *Id.* at 811–12.

243 *Id.*

244 *Id.* at 816–17.

2. *Payment System Complaint Program*[245]

Even though payment intermediaries may not be required to take steps against online copyright infringement, they have chosen to do so.[246] This Section describes the policy behind this activity and one example of such action. The payment intermediaries go beyond their legal duty for a variety of business reasons. Being associated with illegal activity is harmful to their brands. Responding to complaints from reputable businesses about losses from illegal activities strengthens a payment intermediaries' reputation as a responsible business partner. It also lends credence to the intermediaries' oft-repeated assertions that their payment systems should not be used for illegal activities. By keeping it free of illegal activity, the payment networks promote trust in electronic commerce, a channel of commerce in which they have a competitive advantage over traditional payment mechanisms like cash and check.[247]

How did payment systems take on the challenge of responding to complaints of copyright infringement? Payment systems cannot monitor their networks for copyright law violations. They do not have the factual basis to conclude that a particular sale of a product is a violation of someone's copyright.[248] Many music downloads are perfectly legal transactions, but some are not. Distinguishing the two is often a complex factual and legal question which payment intermediaries do not have the expertise or ability to resolve.

For this reason a coding and blocking system like the one used to address internet gambling will not work.[249] Merchants' transactions are coded by business category, not legal status.[250] If financial institutions blocked transactions based on the business code for a music download, they would block a substantial number of legal transactions. Since copyright owners benefit from these legal transactions, they would not want an overly broad coding and blocking scheme.

---

[245] Portions of this Section are taken directly from the author's congressional testimony, as cited.

[246] *See generally International Piracy: The Challenges of Protecting Intellectual Property in the 21st Century: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 110th Cong. 73–82 (2007) [hereinafter *International Piracy Hearing*] (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.) (providing this account of payment intermediaries and intellectual property).

[247] *Id.* at 75.

[248] *Id.* at 76.

[249] *See supra* Section III.A (discussing the internet gambling coding and blocking scheme).

[250] VISA MERCHANT CATEGORY CLASSIFICATION (MCC) CODES DIRECTORY, *supra* note 105.

A coding and blocking scheme for copyright would also be inappropriate because the international legal status of copyright differs from the international legal status of internet gambling. Internet gambling is illegal in some jurisdictions. For that reason, one could require merchants to properly code themselves and to allow financial institutions in countries where internet gambling is illegal to block these labeled transactions. But internet merchants involved in illegal intellectual property infringement typically violate the laws of most countries.[251] 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.

Therefore, 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.

The payment systems have to react to complaints of copyright violations because they cannot monitor for them on their own. They cannot take proactive steps as they could in the case of child pornography or controlled substances.[252] The payment networks have thus developed policies and procedures to handle these complaints.[253] 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.[254]

The complaint process starts when a business entity approaches a payment system with clear, documented evidence of illegal activity and adequately identifies the infringing internet merchant.[255] The business entity must provide substantiation that the activity is illegal and documentation that payment cards are actually being used for this illegal activity.[256]

The next step is to assess legality. This is easier if there is regulatory or judicial precedent establishing the illegality, but that is rare. If the buyer and the seller are in the same jurisdiction, this legal assessment can be relatively

---

[251] *International Piracy Hearing*, *supra* note 246, at 77 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

[252] *See supra* Sections III.B.1, III.B.2.

[253] *International Piracy Hearing*, *supra* note 246, at 77 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

[254] *Id.*

[255] This Section describes the process at Visa, but other payment networks use a similar process. *See id.* at 85.

[256] *Id.*

straightforward.[257] But these cases are not typical because companies tend to pursue domestic remedies for domestic cases. They usually come to payment networks only 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 when the merchant is in one jurisdiction, the customer is 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, the assessment is far more complex.[258]

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.[259] In cases like copyright infringement, this means that merchants are responsible for making sure that the transactions they submitted to the payment system are legal in both their operating jurisdiction and the jurisdiction in which their customer is located.

The assessment of legality requires the payment network to determine whether the type of transaction would be illegal in either jurisdiction.[260] Since the facts and law involved are often complex, the payment networks are willing to take on only the clearest cases of copyright violation. Once they determine illegality, 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, and providing the complaint to the bank involved usually resolves the issue.[261] In most cases, either the bank does not want the business and terminates the merchant, or it takes other action to bring the merchant into compliance.[262] If the bank does not take action, the payment networks can take further enforcement action against the bank.[263]

3. Allofmp3.com

In some instances, the merchant resists the enforcement efforts of payment systems, and insisting on the legality of the underlying activity, the merchant goes to a local court to vindicate its perceived rights under local law. This is what occurred in the Allofmp3.com case.

As part of its general policy on cross-border transactions, Visa concluded that it did not want this type of transaction—illegal downloads of music—in

257 *Id.* at 77.
258 *Id.* at 77–78.
259 *Id.* at 78.
260 *Id.*
261 *Id.*
262 *Id.*
263 *Id.*

its payment system.[264] This decision enabled it to extend enforcement actions against this one site to different sites or to the same site processed by a different bank.

In 2005, Visa received a documented complaint from International Federation of the Phonographic Industry (IFPI), which represents copyright owners based in more than seventy countries.[265] The complaint alleged that Allofmp3.com, a website located in Russia, was infringing on the copyrights of IFPI's members by allowing unauthorized downloads of music.[266] Visa assessed the legal situation, in part by obtaining a review by outside counsel, and concluded that the transactions were illegal under local Russian law.[267] They were also illegal under the laws of the vast majority of the merchant's customers who were located primarily in the United Kingdom and the United States.[268] In October 2005, the Italian authorities shut down a portal to Allofmp3.com, allofmp3.it, and began a criminal investigation of the Italian site.[269] In addition, the United States Trade Representative intervened with the Russian government to urge them to shut down Allofmp3.com.[270]

At the beginning of September 2006, after appropriate notice, the Russian bank working with Allofmp3.com stopped processing Visa transactions for Allofmp3.com.[271] At the end of September 2006, the bank also stopped processing transactions from an affiliated site called allTunes.[272] After these Visa transactions ended, further confirmation of the site's illegality was 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.[273] MasterCard also cut off

---

264 *Id.* at 79.

265 *Id.*

266 *Id.* (discussing IFPI's role); Nate Anderson, *Music Industry Encouraged Visa to Pull the Plug on AllofMP3.com*, ARSTECHNICA, Oct. 19, 2006, http://arstechnica.com/business/news/2006/10/8029.ars.

267 *International Piracy Hearing*, *supra* note 246, at 79 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

268 *Id.*

269 Press Release, IFPI, Allofmp3.com: Setting the Record Straight (June 2, 2006), *available at* http://www.ifpi.org/content/section_news/20060601.html.

270 *See International Piracy Hearing*, *supra* note 246, at 26 (testimony of Victoria A. Espinel, Assistant U.S. Rep. for Intellectual Property and Innovation, Office of the U.S. Trade Rep.) ("We will continue to press Russia to shut down and prosecute the operators of illegal Web sites operating in Russia, including the successors to the infamous AllOfMP3.com.").

271 *Id.* at 79 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

272 *Id.*

273 Press Release, IFPI, New Court Setback for Allofmp3.com (Oct. 26, 2006), *available at* http://www.ifpi.org/content/section_news/20061026.html.

payment services to allofmp3.com.[274] By May of 2007, the site's popularity had plummeted.[275]

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.[276] Visa was a party to that litigation on the side of the bank.[277] In June 2007, the owner won a judgment that the bank had violated its contract with the merchant, and the judgment required the bank to continue to provide processing services.[278] 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 rights holders.[279]

In August 2007, another Russian court issued a ruling in a different case, relating to criminal copyright infringement initiated by IFPI against the owner of Allofmp3.com.[280] This ruling stated that there had not been sufficient confirmation of any illegal activity by the site's owner.[281] Even though the copyright owners had not given permission to distribute their recorded material, a Russian collective rights society (the Russian Multimedia and Internet Society, or ROMS by its initials in Russian) was deemed to be operating legitimately under Russian law.[282] The court implied that Allofmp3.com and similar sites would be in compliance with Russian law to the extent that they paid for rights from this Russian collective rights society.[283]

---

[274] *MP3 Site's Voucher System Closes*, BBC NEWS, May 21, 2007 *available at* http://news.bbc.co.uk/2/hi/entertainment/6677265.stm.

[275] IFPI reported in May 2007 that Allofmp3 "rated outside the top 2000 websites." Press Release, IFPI, Police Dawn Raid Stops Allofmp3.com Pirate Vouchers Scheme (May 21, 2007), *available at* http://www.ifpi.org/content/section_news/20070521.html.

[276] Arbitration Court of Moscow 2007, A40-70411/06-67-500.

[277] *Id.* at 1.

[278] *Id.* at 5.

[279] *Id.* The court stated,

> 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.

Id. The Defendant was Rosbank, the Russian financial institution licensed by Visa to authorize merchants in Russia to accept Visa. *Id.*

[280] Cheremushkinsky [District Court of Moscow], 2007, No. 1-151-07.

[281] *Id.* at 4.

[282] *Id.* at 5.

[283] *Id.*; *see also International Piracy Hearing*, *supra* note 246, at 99 (testimony of Victoria A. Espinel, Assistant U.S. Rep. for Intellectual Property and Innovation, Office of the U.S.

These court cases created a challenge for Visa because the payment system had responded to a documented complaint of copyright infringement.[284] 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.[285] 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.[286] Transactions from customers in other countries would not be allowed.[287]

4. Assessment of Payment System Actions on Online Copyright Infringement

The actions of payment systems to limit use of their systems for copyright infringement can be evaluated using the framework set out in Part II by examining the equities, market, and costs and benefits that would be involved if public policy imposed intermediary liability.

First, *Perfect 10* properly rejected indirect liability for payment intermediaries.[288] 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 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? Unintentionally, Judge Kozinski's dissent brought out this implication.[289]

Trade Rep.) ("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.").

284 *Id.* at 80 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

285 *Id.* at 80–81.

286 *Id.*

287 *Id.* at 81.

288 Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 798 (9th Cir. 2007). For analysis, see Band, *supra* note 231.

289 *See id.* at 824 (Kozinski, J., dissenting) ("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 id.* Kozinski argues that

> [p]laintiff 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 . . . be the end of Capitalism as we know it.

Id. But it might be the end of payment systems as we know them if indirect liability for them

Judge Kozinski also painted a clear picture of how, in his opinion, payment intermediaries might act if they were liable for copyright infringement occurring through their services:

> [T]he 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.[290]

Judge Kozinski contemplated that the U.S. based payment intermediaries could more easily take action against parties in other jurisdictions compared to other actors: "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."[291]

But the actual experience of payment intermediaries reveals that things would not be that simple.[292] Even in the case of a well documented complaint, payment intermediaries are never truly asked to remove "infringing" material.[293] At best, there is a well-documented assertion of infringement under the laws of a particular jurisdiction.[294] Judge Kozinski appears to favor a notice-and-takedown approach, so that payment intermediaries are not responsible for illegal conduct of which they are unaware.[295] But as Visa found in *Allofmp3.com*, payment card services and their associated financial service partners can be liable for wrongful

means an obligation to stop doing business with everyone who might be involved with illegality anywhere. Kozinski attempts 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. *Id.* at 819–20. 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?

290 *Id.* at 817.

291 *Id.* at 823.

292 *See supra* Section III.C.3.

293 *See supra* Section III.C.3.

294 *See supra* Section III.C.3.

295 *Perfect 10*, 494 F.3d at 824 (Kozinski, J., dissenting).

termination of services in those jurisdictions if they react to an allegation of infringement by "kick[ing] the pirates off their payment networks."[296]

Second, there is no market failure in this situation that would justify imposing intermediary liability on payment systems. There are available arrangements between payment intermediaries and copyright owners that can reduce the amount of copyright infringement on the Internet.[297] These arrangements are informal, but expanding. They rely on complaints by copyright owners, followed by investigation and action by intermediaries.[298] They seem to strike a cost-based balance by putting the burden of discovering infringement on the copyright owner and triggering action by the third party only after notification. The arrangements may involve compensating payment intermediaries for performing enforcement services, but if this enables copyright owners to reduce the harm of copyright infringement, they might very well pay. If there are extra efforts, above and beyond standard practices, that a particular copyright owner would like payment intermediaries to make, those efforts should be open to negotiation. There do not seem to be any transaction costs that would prevent the parties from negotiating adjustments to these arrangements over time. And there appears to be no market failure that would justify not relying on private sector enforcement arrangements.

Third, given the legal risks involved, copyright owners should be willing to indemnify payment intermediaries for damages resulting from enforcement actions against alleged infringers. *Allofmp3.com* indicates that these legal risks are not hypothetical.[299] If the copyright owner is persuaded of the legal soundness of his case, he should be prepared to assume the risk.

---

296 *Id.* at 817. Mann and Belzley's argument 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, 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 better situated, because of the real world likelihood that none of the sites that fosters the infringement could survive as a profitable commercial enterprise without accepting Visa payments.

Mann & Belzley, *supra* note 8, at 264. 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.

297 *See supra* Section III.C.3.

298 *See supra* Section III.C.3.

299 *See supra* Section III.C.3.

It might be one way to assure that only strong complaints are brought to the attention of the payment intermediary. An additional mechanism might be to require the presence of a court or governmental agency that holds that the activity involved is infringing.

A statute could potentially help provide legal immunity to payment intermediaries when they take good faith action against alleged infringers. But U.S. law cannot provide immunity in other jurisdictions, which is where the aid of global payment intermediaries is needed.[300]

Fourth, this case illustrates the need for greater clarity in the legal environment in which intermediaries operate. Intermediaries cannot be in the position of creating new global law through their own interpretation of current statutes. Again, *Allofmp3.com* suggests the need for even greater harmonization of local laws that intermediaries are expected to enforce.[301] The United States Trade Representative attempted this by working with the Russian government to bring about changes in Russian law that would bring it closer to the international norm.[302]

In sum, the experience of payment intermediaries indicates that some efforts on their part to respond to legitimate complaints would be justified. It is not appropriate to do nothing in response to allegations of copyright infringement. The current complaint procedure and case-by-case response is reasonable. It could be improved through further discussions among the parties, further recourse to court judgments of infringement, and harmonization of current international standards.

IV. INTERNET GOVERNANCE

Parts II and III laid out a framework for analyzing intermediary liability and applied it to the actions of payment intermediaries. That analysis is also relevant to fundamental questions of internet governance. This Part explores the extent to which the experience of payment systems in controlling the illegal online behavior of their users illuminates the debate between the internet exceptionalists, defenders of the bordered Internet, and the

300 *See supra* Section III.C.3.

301 *See supra* Section III.C.3.

302 OFFICE OF THE U.S. TRADE REPRESENTATIVE, EXECUTIVE OFFICE OF THE PRESIDENT, RESULTS OF BILATERAL NEGOTIATIONS ON RUSSIA'S ACCESSION TO THE WORLD TRADE ORGANIZATION (WTO): ACTION ON CRITICAL IPR ISSUES (2006) ("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 International Piracy Hearing*, *supra* note 246, at 30 (statement of Victoria A. Espinel, Assistant U.S. Rep. for Intellectual Property and Innovation, Office of the U.S. Trade Rep.).

internationalists. It concludes that exceptionalism, in either its original or modified forms, is not the right framework for internet governance because intermediaries should not defer to the judgments of self-governing communities of internet users when the judgments conflict with local law. The exceptionalists are correct that a "bordered Internet" will not scale up, but the experience of traditional payment systems points towards international harmonization. If governments are going to use intermediaries to regulate the Internet, they need to coordinate their own laws to make that role possible.

This Part addresses each of the three main approaches to internet governance: exceptionalism, the bordered Internet, and internationalism. Section IV.A, on exceptionalism, begins with a discussion of 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. This is followed by a discussion of Brian Holland's revised version of exceptionalism. Under this approach, the various immunities from intermediary liability established by local jurisdictions enable the development of autonomous Internet norms. Both versions are shown to have significant limitations when viewed in light of payment system experiences. Section IV.B explores the "bordered Internet," the idea that in certain cases local governments may properly and unilaterally extend their jurisdiction over internet activities through intermediaries. Payment intermediaries use standard measures to resolve conflicts of law and follow a practical rule that treats a transaction as illegal if it is illegal in the jurisdiction of either the merchant or the cardholder. Section IV.B then discusses limitations on this method of resolving cross-border jurisdictional conflicts. Section IV.C concludes with a discussion and endorsement of the internationalist perspective, according to which local governments should only exercise control over specific internet activities in a coordinated fashion.

A. INTERNET EXCEPTIONALISM

1. The Original Version

In February 1996, John Perry Barlow identified internet exceptionalism when he 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."[303] Conflicts in cyberspace would be resolved not with the

[303] Declaration of John P. Barlow, Cognitive Dissident, Co-Founder, Elec. Frontier Found., A Declaration of the Independence of Cyberspace (Feb. 8, 1996), *available at* http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

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."[304] Rather, in cyberspace "governance will arise according to the conditions of our world, not yours."[305] Cyberspace "is different."[306]

Almost concurrently, legal scholars David Johnson and David Post made a similar case for internet exceptionalism.[307] 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 a local sovereign's efforts to regulate global phenomena . . . ."[308] 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."[309] The Internet destroys the legitimacy of local jurisdiction because legitimacy depends on the consent of the governed and "[t]here is no geographically localized set of constituents with a stronger and more legitimate claim to regulate it than any other local group. The strongest claim to control comes from the participants themselves, and they could be anywhere."[310] Since "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."[311]

Behind these arguments seemed to be an appealing political vision. The ideal envisaged self-organizing groups of people making 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 in practice had long failed to provide their members with the sense of

304 *Id.*
305 *Id.*
306 *Id.*
307 *See generally* Johnson & Post, *supra* note 1.
308 *Id.* at 1370 (emphasis added).
309 *Id.* at 1374.
310 *Id.* at 1375.
311 *Id.* at 1376.

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 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.[312] It is hard to avoid the sense that the political vision predated the Internet—that the feasibility argument masked the underlying vision and 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

312 Mann and Belzley describe 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 because of the ease of identifying intermediaries, the relative ease of intermediary monitoring of end users, and the relative difficulty of directly regulating the conduct of end users." Mann & Belzley, *supra* note 8, at 250–51. 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 and Belzley'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.

not feasibility of control, but the value of participative community decision making and diversity.

This early cyber libertarian vision was immediately attacked by those who defended the feasibility and legitimacy of extending local laws to cover internet activity.[313] As they note, "[t]he 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."[314] Government action against these intermediaries "makes it harder for local users to obtain content from, or transact with, the law-evading content providers abroad. In this way, governments affect Internet flows within their borders even though they originate abroad and cannot easily be stopped at the border."[315] 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 can usually be provided only by governments." [316]

This attack was so effective that many believe that these notions of a "self-governing cyberspace are largely discredited."[317] But modified versions accept the basic premise that the Internet should be free of local regulation and governed by its users. One version of the revived exceptionalism, defended by Brian Holland, focuses on Web 2.0 communities.[318] This view argues that together with the immunity provisions of § 230 of Communications Decency Act, these communities have the potential to allow internal community norms to take the place of external territorially based laws.[319]

---

313 *See generally* Goldsmith, *supra* note 2 (challenging the regulation skeptics).

314 Goldsmith, *supra* note 2, at 1238.

315 GOLDSMITH & WU, *supra* note 7, at 68.

316 *Id.* at 140.

317 *Id.* at 14.

318 Holland writes,

> By mitigating the imposition of certain external legal norms in the online environment, § 230 helps to create the initial conditions necessary for the development of a modified form of exceptionalism. With the impact of external norms diminished, Web 2.0 communities, such as wikis and social networks, have emerged to facilitate a limited market in norms and values and to provide internal enforcement mechanisms that allow new communal norms to emerge.

Holland, *supra* note 16, at 369.

319 *Id.*

2. *Critique of Internet Exceptionalism*

The experience of global payment intermediaries described in Part II confirms the view that intermediaries can effectively control illegal activity in cyber space. This still leaves the question of whether intermediaries should resist such attempts to control the behavior of their users. As a general matter, they should not defer to the judgments of self-governing communities of internet users when these judgments conflict 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. But even when local law does not require them to take action against illegal behavior, as in the child pornography, controlled substances, and online tobacco cases described earlier, their responsibility to keep their systems free of illegal activity means that they often should take specific steps to stop these activities.

The fundamental objection, even to Holland's modified exceptionalism, is that 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, and the terms of the contract are subject to the same kinds of legal and regulatory oversight that bind contracts between people in local jurisdictions. Deferring to these contracts does not usually mean democratic community self-government. Local regulations are needed to fully protect the members of these communities.[320] Moreover, in some cases the legal discretion granted to intermediaries to control the conduct of their members may be too broad and should be limited by replacing intermediary judgment with public authority decisions. The remainder of this Section develops these points.

Even if internet communities could substantially exclude a significant portion of external legal norms, it still does not imply that internal norms will emerge from the 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."[321] 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, allowing users to establish norms for their own communities.[322]

---

[320] This Section focuses on competition policy, privacy, and consumer protection as examples.

[321] Holland, *supra* note 16, at 398.

[322] These internal incentives include "the need for financial support from community

But it is not clear that Web 2.0 platforms are likely to grant this kind of democratic self-governance. For example, 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.[323] 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.[324] One could argue immunity in this case, but Craigslist did not.[325] It complied with a law enforcement request to remove certain postings and the decision to remove these ads will be subject to ongoing oversight by these law enforcement agencies.[326] However, the question remains whether or not Craigslist would take the legal risk if the community voted to keep these ads in place.

These communities are not typically governed by democratic voting procedures that guarantee the consent of the governed. They are governed by contractual terms of service. Often prospective members of these communities have a simple take-it-or-leave-it choice when they decide to join.[327]

---

donations, a communal desire for information integrity, or the need to build an audience for advertising." *Id.* at 400; *see also* Schruers, *supra* note 68, at 261 ("ISPs respond to content-based complaints as a matter of good business practice for the purpose of maintaining customer goodwill and satisfaction.").

323 Craigslist Founder Seeks Larger DC Role, NAT'L J., June 2, 2009, *available at* http://techdailydose.nationaljournal.com/2009/06/craigslist-founder-seeks-large.php (reporting Craig Newmark's comments to the Computers Freedom and Privacy Conference).

324 *See* Brad Stone, *Craigslist to Remove 'Erotic' Ads*, N.Y. TIMES, May 14, 2009, at B1. Craigslist's attorneys asserted immunity under § 230, but chose voluntarily to remove the ads to which various state attorneys general had objected. *Id.* State Attorneys General felt confident that they could bring a case under state criminal law despite the immunity granted by § 230. *Id.* The case was given national attention when a medical student was accused of killing a masseuse whom he met through Craigslist. *Id.*

325 *Id.*

326 *Id.*

327 *See* Johnson & Post, *supra* note 1, at 1380 (describing AOL or Compuserve terms of service as examples of law in cyberspace). Johnson and Post view the rules for an internet community to be "a matter for principled discussion, not an act of will by whoever has control of the power switch." *Id.* 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 the service or application. It might satisfy certain legal standards for informed consent, but it is not the product of principled discussion. 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 many 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 websites they visited just

If consumers do not like the terms of service, then protest can be effective, as 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 stirred up substantial community unrest, and ultimately the new terms of service were withdrawn.[328] But this exit right is not the same as democratic self-governance, and it is not always effective. What if Facebook had not responded to community objections? Would people actually have left, and where would they have gone? Lock-in is a real phenomenon in social networks.

The exemption from liability based on § 230 does not mean that online entities are exempt from local law. Often, local law is needed to protect consumers from the actions of internet intermediaries. Regulation of online communities by governments seems especially timely and urgent in three areas—competition policy, privacy, and consumer protection.

With respect to competition, concentration in particular sectors of the online world should 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.[329] Along with the FTC, they have initiated inquiries focused on the search engine market.[330]

Privacy and security rules need to be defined as well. The FTC has taken major action in this area, and is stepping up their enforcement.[331] They are

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. Aleecia M. McDonald & Lorrie F. Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 565 (2008).

328 N.Y. Times, Facebook, Inc., http://topics.nytimes.com/top/news/business/companies/facebook_inc/index.html (last updated May 27, 2009). In 2007, the company had created a community backlash when it introduced an advertising service that allowed a user's online activities to be distributed to other community members. Epic.org: Electronic Privacy Information Center, Social Networking Privacy, http://epic.org/privacy/socialnet/default.html (last visited Feb. 3, 2009). In the face of this protest, it provided a simple way for users to decline to participate. *Id.* 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. *Id.*

329 Press Release, U.S. Dep't of Justice, Justice Department Withdraws Report on Antitrust Monopoly Law: Antitrust Division to Apply More Rigorous Standard with Focus on the Impact of Exclusionary Conduct on Consumers (May 11, 2009), *available at* http://www.justice.gov/atr/public/press_releases/2009/245710.pdf.

330 *See, e.g.*, Miguel Helft, *U.S. Inquiry Is Confirmed into Google Books Deal*, N.Y. TIMES, July 3, 2009, at B3; Miguel Helft & Brad Stone, *Board Ties at Apple and Google Scrutinized*, N.Y. TIMES, May 5, 2009, at B1; Peter Whoriskey, *Google Ad Deal Is Under Scrutiny: Yahoo Agreement Subject of Antitrust Probe, Sources Say*, WASH. POST, July 2, 2008, at D1.

331 *See* Press Release, Fed. Trade Comm'n, Sears Settles FTC Charges Regarding Tracking Software (June 4, 2009), *available at* http://www.ftc.gov/opa/2009/06/sears.shtm

also focusing on the development of a new privacy framework to analyze the basis for the harms associated with privacy violations.[332] Furthermore, the FTC has focused on developing rules for online behavioral advertising.[333] In addition, rules governing privacy for online cloud computing services need to be clarified, perhaps by additional legislation.[334]

Consumer protection rules should be updated to apply more effectively to new developments in electronic commerce including the growth of mobile commerce and user-generated content, the greater availability of digital goods online, and increased numbers of consumers acting 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.[335]

Finally, the discretion given to internet intermediaries over which transactions to allow must be subject to public scrutiny. Today, intermediaries exercise judgment 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, explained above, 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.

(reporting that in the Sears case the FTC 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).

332 *See* Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 5, 2009, at B1 (stating that David Vladek, the new head of the FTC's consumer protection division, is rethinking privacy). Vladek said that "[t]he frameworks that we've been using historically for privacy are no longer sufficient." *Id.* 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, "[t]here's a huge dignity interest wrapped up in having somebody looking at your financial records when they have no business doing that." *Id.*

333 *See* Press Release, Fed. Trade Comm'n, FTC Staff Revises Online Behavioral Advertising Principles (Feb. 13, 2009), *available at* http://www.ftc.gov/opa/2009/02/behavad.shtm.

334 *See generally* ROBERT GELLMAN, WORLD PRIVACY FORUM, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING (2009) (discussing these cloud computing issues).

335 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.

- Payment systems take complaints from third parties, 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 choose to adopt lists of dangerous substances from the FDA and DEA lists and determine that they cannot be sold by internet pharmacies.

These decisions are sound and sensible ways to balance complex and competing interests. However, they are 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 January 2009, it was reported that an Irish ISP had agreed to disconnect subscribers who were accused of three instances of infringement by a copyright owner.[336] Allegations of violations would be made by a contractor working for the content owner and transmitted to the ISP.[337] At this point, these decisions are largely up to the payment intermediaries and the ISPs themselves, although in some jurisdictions they are dictated by government requirements,[338] yet their

---

336 Posting of Danny O'Brien to Deeplinks Blog, Irish ISP Agrees to Three Strikes Against Its Customers, http://www.eff.org/deeplinks/2009/01/irish-isp-agrees-three-strikes-against-its-users (Jan. 28, 2009).

337 *Id.* 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. *Id.* As O'Brien 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?

Id.

338 The movement toward graduated response would replace this discretion with government processes. Under the recently passed HADOPI law, French ISPs would be required to suspend internet access for subscribers who have been subject to three allegations of copyright violations. Catherine Saez, *French HADOPI Law, Now Complete, Can Brandish Its Weapons*, INTELL. PROP. WATCH, Oct. 23, 2009, http://www.ip-watch.org/weblog/2009/10/23/french-hadopi-law-now-complete-can-brandish-its-weapons/. A court review would be required before suspension. *Id.* A similar graduated response program was adopted in Britain in April 2010. Eric Pfanner, *U.K. Approves Crackdown on Internet Pirates*, N.Y. TIMES, Apr. 8, 2010, http://www.nytimes.com/2010/04/09/technology/

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.

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."[339] To the extent that an internet community is self-contained or its activities affect others only on a voluntary basis, then there is a case for deferring.[340]

B. PAYMENT SYSTEMS AND THE BORDERED INTERNET

Goldsmith and Wu attack internet exceptionalism, but they also construct a positive vision of a "bordered Internet."[341] This world 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.[342]

Resolving jurisdictional disputes would be one significant problem with the bordered Internet. The initial internet exceptionalist argument was that internet activity is simultaneously present in multiple overlapping and inconsistent jurisdictions, and that no one jurisdiction has a better claim to regulate the 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. Goldsmith and Wu's response was that internet activity was real world activity, taking place in particular jurisdictions, and that local governments

09piracy.html. Whether these graduated response programs are needed is a point of controversy, but they replace ISP discretion with a system of public accountability.

339 Johnson & Post, *supra* note 1, at 1389.

340 *See* POST, IN SEARCH OF JEFFERSON'S MOOSE, *supra* note 15, at 178–86 (describing "massively multi-player online games" or MMOGS as good candidates for this effort at online rule creation). This might be. However, Linden Labs, the creator of one of the famous MMOGs, found it necessary to rely on external banking regulators when it decided to ban the offering of interest or any return on investment in-world without proof of an applicable government registration statement or financial institution charter. Posting of Kend Linden to Second Life Blogs, New Policy Regarding In-World "Banks", https://blogs.secondlife.com/community/features/blog/2008/01/08/new-policy-regarding-in-world-banks (Jan. 8, 2008 06:43:56 PM). Linden Labs properly concluded that it "isn't, and can't start acting as, a banking regulator." *Id.* 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.

341 GOLDSMITH & WU, *supra* note 7, at viii.

342 *Id.* at 149.

could exert control over this activity by attaching obligations to the local operations of global internet intermediaries.[343] This indirect liability for intermediaries would make it easier to extend local law to the bad actor.[344] Conflict of laws would be handled by the normal mechanisms for resolving these disputes, and ultimately enforced by actions taken against local operations of global intermediaries.[345]

Jurisdiction in cyberspace is a complex topic with many different approaches to assigning both the applicable law and the court of jurisdiction.[346] Questions include determining the location of the transaction, the jurisdiction, and the interests of the parties.[347] An early attempt to deal with these issues in the internet context was the Federal Trade Commission's (FTC) approach to consumer protection in the global marketplace.[348] The simplest cross-border electronic transaction implicates transnational concerns. Choice of law debates inevitably follow. The FTC considered arguments for the "country of origin" approach and the "country of destination" approach.[349] 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.[350] Under the country of destination approach, the law of the consumer would apply and the courts of the consumer's country would adjudicate disputes.[351]

---

343 *Id.* at 68–72.

344 Mann & Belzley, *supra* note 8, at 259 ("[On the Internet it is] easier for even solvent malfeasors engaged in high-volume conduct to avoid responsibility either through anonymity or through relocation to a jurisdiction outside the influence of concerned policymakers."). Mann and Belzley also argue that indirect liability makes sense in "cases in which the retailer is located in a jurisdiction outside the United States that will not cooperate with the relevant state regulators." *Id.* at 277.

345 GOLDSMITH & WU, *supra* note 7, at 158–61.

346 *See, e.g.*, Paul S. Berman, *Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era*, 153 U. PA. L. REV. 1819, 1822 (2005) (arguing that judges should adopt a cosmopolitan approach in internet cases involving choice of law and foreign judgment issues, grounded in the "idea that governments have an interest not only in helping in-state litigants win the particular litigation at issue, but a more important long-term interest in being cooperative members of an international system and sharing in its reciprocal benefits and burdens").

347 *See generally* Goldsmith, *supra* note 2 (discussing many of these theories); *see also* Berman, *supra* note 346, at 1839–40 (discussing various choice-of-law theories that address these questions).

348 FED. TRADE COMM'N, CONSUMER PROTECTION IN THE GLOBAL ELECTRONIC MARKETPLACE: LOOKING AHEAD (2000). The FTC's discussion of applicable law and jurisdiction is especially relevant. *Id.* at 4–11.

349 *Id.*

350 *Id.* at 2.

351 *Id.* The European Union appeared to take the side of the country of origin in its E-Commerce Directive. European Commission, E-Commerce Directive, http://ec.europa.

The defense of the country of origin approach relied on the difficulty of applying any other legal framework to the electronic marketplace.[352] Only this country of origin framework seems to allow for the growth of global e-commerce. The framework considers problems encountered by small businesses selling in many countries of creating and applying a standard for some variety of "purposeful" targeting. Creating a default rule of the country of origin was deemed to better provide needed uniformity and predictability for online businesses.

This approach has defects. First, it forces consumers to rely on unfamiliar consumer protections. If merchants cannot be expected to know the laws of 180 countries, neither can consumers. Second, it creates a race to the bottom, whereby unscrupulous merchants can 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 suffice. 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.[353] For other issues that could not be addressed through these means, the traditional tools of international conflict of law resolution would have to suffice.[354]

---

eu/internal_market/e-commerce/directive_en.htm (last visited Feb. 15, 2010). The 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." *Id.*

[352] FED. TRADE COMM'N, *supra* note 348, at 4 (discussing the "two fundamental challenges" to a country-of-destination framework, including "the use of physical borders to determine rights in a borderless medium" and compliance costs).

[353] 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. ORG. FOR ECON. CO-OPERATION & DEV., GUIDELINES FOR CONSUMER PROTECTION IN THE CONTEXT OF ELECTRONIC COMMERCE (1999) [hereinafter OECD GUIDELINES], *available at* http://www.oecd.org/document/51/0,3343,en_2649_34267_1824435_1_1_1_1,00.html.

[354] 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 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

Some commentators, such as Paul Berman, attempted to reach beyond the traditional dispute resolution mechanisms for resolving conflict of law cases with principles that take into account the realities of multiple community affiliations.[355] 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.[356] 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 according to a series of principles that recognized the need to balance competing national norms.[357]

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 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, discussed in Section III.A, was that a transaction is unacceptable in the payment system if it is illegal in the jurisdiction of either the buyer or the seller.[358]

The payment card approach provides a simple default rule for intermediaries to apply when determining whether to allow transactions in their systems. It eliminates the heavily fact-based balancing assessments needed to determine, on a case by case basis, whose law applies. The default rule also does not simply adopt a country of origin or country of destination

> 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.

Holland, *supra* note 16, at 393.

355 Berman, *supra* note 346, at 1862.

356 *Id.*

357 *Id.* Berman's work has affinities with that of political philosophers working in the area of national sovereignty in a global world. *See, e.g.*, POGGE, *supra* note 82, at 168–95.

358 Visa's policy is stated in *International Piracy Hearing*, *supra* note 246, at 71 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.). Other payment intermediaries have similar procedures, such as eBay's restriction about selling and shipping illegal goods to the country where they are illegal. eBay, Offensive Material Policy, http://pages.ebay.com/help/policies/offensive.html (last visited Feb. 4, 2010) ("[B]ecause 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.").

perspective, each of which is limited. Nor does it leave the transaction in a legal limbo where no law applies.[359]

The payment system experience leads to several observations. First, direct conflicts of law are not as frequent as some anticipated. 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.[360]

Second, regulating the Internet by 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

[359] 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 U.S. 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, as discussed earlier in this Article. 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.

[360] *See, e.g.*, Press Release, Privacy Int'l, Europe's Privacy Commissioners Rule Against SWIFT (Nov. 23, 2006), *available at* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-546365 (describing the SWIFT case, where SWIFT was required to comply with U.S. demands for access to financial information about European customers in virtue of its operations on U.S. soil, while such compliance put them in violation of the European data protection directive). In addition, passage of the Global Online Freedom Act (GOFA) could put internet intermediaries in a conflict of law situation with China and other countries. *See* Global Online Freedom Act of 2007, H.R. 275, 110th Cong. (2007). H.R. 275 was introduced by Representative Chris Smith on January 5, 2007 and would require U.S. intermediaries to resist certain orders from countries in which they are doing business. *Id.*

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 thus nothing to which normal mechanisms of conflict resolution may attach.[361]

Some commentators have correctly pointed out that when the laws of different jurisdictions apply to a single transaction, the ability of any particular jurisdiction to unilaterally regulate the Internet is limited.[362] But intermediaries can reduce these conflicts. Global payment systems can simplify transactions to events in which only a buyer in one jurisdiction and a seller in another are implicated. By concentrating enforcement in intermediaries instead of individuals or merchants, local jurisdictions can take advantage of the economies that these institutions make possible.

The experience of payment intermediaries reveals that, within limits, the differences among conflicting jurisdictions can be managed. The bordered Internet works on a small scale. The scale is currently 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. Moreover, in contrast to the rhetoric about the Internet creating a global marketplace, the scope of cross-border commerce itself is still limited. The reality is that the volume of cross-border transactions is not large enough to create a truly substantial cross-border jurisdictional crisis. Currently, only four percent of the sales for electronic commerce merchants in the U.S. come from abroad.[363] And data from Europe show that cross border online transactions are not increasing as fast as overall e-commerce transactions, staying relatively stable from 2006 to 2008 at six to seven percent.[364]

---

[361] Antigua brought a complaint against the U.S. for the enforcement of its gambling laws, but its success was based only on (1) the U.S.'s failure to exclude internet gambling from the list of services that required open treatment and (2) the idiosyncrasies of U.S. 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 U.S. law and international WTO law and are not real conflict of law problems. *See* Appellate Body Report, *supra* note 130, 358–64.

[362] *See, e.g.*, H. Brian Holland, *The Failure of the Rule of Law in Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty*, 24 J. MARSHALL J. COMPUTER & INFO. L. 1, 26 (2005).

[363] This is based on transaction data from the Visa system. *See International Piracy Hearing*, *supra* note 246, at 75 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

[364] Comm'n of the European Cmtys., *Commission Staff Working Document: Report on Cross-Border E-commerce in the EU* 3, SEC (2009) 283 final (Mar. 5, 2009), *available at* http://ec.europa.eu/consumers/strategy/docs/com_staff_wp2009_en.pdf ("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%).").

As David Post has warned, the problem the Internet creates for local jurisdictions is one of scale.[365] The bordered Internet simply does not scale up. 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.

It is not hard to see how a "tragedy of the commons" could arise 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. However, one of two outcomes will occur as the cross-border rules pile up: 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 e-commerce activities of other countries will mount. Either development reveals the limitations of the bordered Internet as a long-term framework for internet governance.

Goldsmith and Wu suggest that enforcement of internet regulations through intermediaries is necessarily limited in size.[366] They suggest that maybe the system will not be able to scale up, but it won't have to.[367] 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.[368] However, there are a sufficiently large number of countries that global intermediaries will not feel capable of abandoning. If all of them use the intermediary enforcement mechanism, the system will be overwhelmed.

---

365 *See* Post, *Against "Against Cyberanarchy"*, *supra* note 15, at 1377 (stating that "scale matters"); *see also* Holland, *supra* note 362, at 29. Holland states,

> 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.

Id.

366 GOLDSMITH & WU, *supra* note 7, at 81–82.

367 *Id.* at 81.

368 *See id.* at 160 (suggesting 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 and thus creating another objection to the bordered Internet to effectively give larger countries a greater role in internet governance than smaller ones).

C. INTERNATIONALISM

The fundamentally correct insight of the internet exceptionalists is that the unilateral imposition of one nation's law onto all internet activities that cross borders won't scale.[369]

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.[370] 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. The basic justification for this policy is similar to the justification for establishing a single uniform national policy that prevents the clash of inconsistent rules at the state 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.[371] This universalism could promise better laws, whereby the "[i]nternational standards could reflect a kind of collection of best practices from around the world—the opposite of the tyranny of the unreasonable."[372]

Goldsmith and Wu make several criticisms of internationalism. First, a system of universal laws would be unattractive; it would leave the world divided and discontent 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,

---

369 *See* Johnson & Post, *supra* note 1, at 1390 ("One nation's legal institutions should not monopolize rule-making for the entire Net.").

370 GOLDSMITH & WU, *supra* note 7, at 26.

371 *Id.* ("If the nations of the world 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.").

372 *Id.* at 27. Reidenberg also argues that as jurisdictions increasingly conflict there will need to be an overarching harmonization of international rules:

> [O]nline 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.

Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213, 230 (2003–2004).

and other considerations 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.[373]

The responses to these criticisms are straightforward. An unpopular global law is not the goal. Neither is 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 also need to take steps to integrate the laws they want to enforce. The reason for this is that global intermediaries' costs 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.[374]

Berman also describes how the internationalist hope for 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."[375] However, he is critical of this universal world community, for two reasons. First, because of its potential to dissolve community affiliations that provide important emotional connections and opportunities for normative discussion of those connections. Second, he views this universal community as fundamentally unrealistic given the dominance of current notions of nation-state sovereignty.[376]

---

373 *See* GOLDSMITH & WU, *supra* note 7, at 152–60.

374 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, *supra* note 2, at 1235.

375 Berman, *supra* note 346, at 1860.

376 *Id.* at 1860–61.

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 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."[377] But participation in global community and the wisdom to know when the global perspective should 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. Similarly, there is no 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.

If governments are going to use payment intermediaries as enforcers of local law, there are a number of steps that could be taken to coordinate their efforts, including:

- In the internet gambling context, a move to an internationally interoperable licensing system that would require 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 internationally accepted list of controlled substances and entities licensed to provide the substances for sale online; and
- In the copyright context, the continued evolution of uniform copyright rules.

377 MICHAEL J. SANDEL, PUBLIC PHILOSOPHY: ESSAYS ON MORALITY IN POLITICS 34 (2005).

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.[378] There are many mechanisms for international coordination. Decisions regarding which mechanisms to use depend 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 there will be no harmonization where there are such fundamental differences. Intermediaries will be called upon to resolve the issue themselves or they 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 superficial 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. For example, the thirty-first International Conference of Data Protection and Privacy Commissioners, held in Madrid in November 2009, adopted a set of global privacy standards.[379] There is also likely to be a renewed push for global consumer protection on the occasion of the tenth anniversary of the Organisation for Economic Co-operation and Development's (OECD)

---

[378] *See* Media Statement, Participants in ACTA Negotiations, Anti-Counterfeiting Trade Agreement (ACTA) (June 12, 2009), *available at* http://www.med.govt.nz/templates/Page____40974.aspx. For a summary of the ACTA process and the content of the agreement, see the Summary of Key Issues. THE ANTI-COUNTERFEITING TRADE AGREEMENT—SUMMARY OF KEY ELEMENTS UNDER DISCUSSION (2009), *available at* http://www.med.govt.nz/templates/MultipageDocumentTOC____40563.aspx.

[379] Artemi R. Lombarte, Dir., Agencia Española de Protección de Datos, Slide Presentation: International Standards on Data Protection & Privacy (2009), *available 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 "[t]o elaborate a set of principles and rights aimed to achieve the *maximum degree of international acceptance*, ensuring at once a high level of protection." *Id.* (emphasis in original). For the standards adopted, see The Madrid Privacy Declaration (Nov. 3, 2009), http://thepublicvoice.org/TheMadridPrivacyDeclaration.pdf.

Guidelines for Consumer Protection in the Context of Electronic Commerce.[380]

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 regardless of 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 a 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 this Article explains, 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 the idea that the Internet was ungovernable because it was a global communications network that crossed borders. This idea 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. Further, the idea that governments cannot control the Internet was undermined by the ability of global intermediaries' local operations to provide essential services and the practical ability of governments to control these intermediaries. Examples from the payment card world demonstrate how this was done in internet gambling, child

---

[380] OECD GUIDELINES, *supra* note 353; *see also* ORG. FOR ECON. CO-OPERATION & DEV., CONFERENCE ON EMPOWERING E-CONSUMERS: STRENGTHENING CONSUMER PROTECTION IN THE INTERNET ECONOMY, PROGRAMME (2009), *available at* http://www.oecd.org/dataoecd/33/22/44045376.pdf (describing the conference). The OECD endorsed steps toward global enforcement of some consumer protection rules in a 2003 report on cross-border fraud and a 2007 report on consumer dispute resolution and redress. *See* COMM. ON CONSUMER POLICY, ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES FOR PROTECTING CONSUMERS FROM FRAUDULENT AND DECEPTIVE COMMERCIAL PRACTICES ACROSS BORDERS (2003), *available at* http://www.oecd.org/dataoecd/24/33/2956464.pdf; COMM. ON CONSUMER POLICY, ORG. FOR ECON. CO-OPERATION & DEV., OECD RECOMMENDATION ON CONSUMER DISPUTE RESOLUTION AND REDRESS (2007), *available at* http://www.oecd.org/dataoecd/43/50/38960101.pdf.

pornography, controlled substances, online tobacco, and copyright infringement.

These examples prove 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 except in extreme cases, they have no right to resist these lawfully established burdens.

Yet, the question remains: should the government place this enforcement burden on intermediaries? The advantages of government intervention sometimes appear to be substantial, but nothing in the least cost arguments suggests 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 imposed unilaterally by local governments would be an improvement. A return to internet exceptionalism would not help matters either.

Greater government coordination on the rules that intermediaries must follow on the Internet would be an improvement. To avoid legal liability and to comply with local laws, payment intermediaries are moving toward accepting the laws of all jurisdictions. They also have wide discretion on what activities to allow on their systems. But this situation is problematic. Intermediaries are not the best-situated to decide which rules to follow. Also, no laws are self-interpreting. They often apply to particular situations in obscure and heavily fact-dependent ways. Intermediaries' flexibility in adjudication leaves room for private, strategic, and unaccountable decisions 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.