Florida Law Review

Volume 67 | Issue 5 Article 1

March 2016

Internet Payment Blockades

Annemarie Bridy

Florida Law Review
Founded 1948

VOLUME 67 SEPTEMBER 2015 NUMBER 5

INTERNET PAYMENT BLOCKADES

Annemarie Bridy[*]

Abstract

Internet payment blockades are an attempt to enforce intellectual property rights by "following the money" that flows to online merchants who profit from piracy and counterfeiting. Where corporate copyright and trademark owners failed in the legislature and the judiciary to create binding public law requiring payment processors like MasterCard and Visa to act as intellectual property enforcers, "non-regulatory" intervention from the executive branch secured their cooperation as a matter of private ordering. The resulting voluntary best practices agreement prescribes a notice-and-termination protocol that extends the reach of U.S. intellectual property law into cyberspace, to merchants operating "foreign infringing sites." It also privatizes the adjudication of infringement claims, raising issues of fairness and institutional competence. Like other forms of regulation by online intermediaries, payment blockades are subject to circumvention through disintermediation. Marrying peer-to-peer (P2P) technology with financial transactions, P2P virtual currencies like Bitcoin allow online merchants and their customers to work around payment blockades.

* Professor of Law, University of Idaho College of Law and Affiliate Scholar, Stanford University Center for Internet and Society (CIS). This paper was initially presented at the 2013 Works in Progress for Intellectual Property (WIPIP) conference, held at Santa Clara Law School. It has benefited from the feedback of WIPIP participants. I would like to thank Mark Bartholomew, Stacey Dogan, and David Post for insightful comments and suggestions on an earlier draft. I owe thanks, too, to Ann Bartow and Stacey Dogan for generous Jotwell reviews, and to Diana Gleason for assistance in obtaining primary documents.

INTRODUCTION

In August of 2010, Pentagon officials publicly threatened reprisals against Julian Assange and his website, WikiLeaks, over the site's publication of leaked military and diplomatic documents, many of them containing information embarrassing to the U.S. government.[1] Less than a week later, the U.K.-based payment processor Moneybookers (now rebranded as Skrill) stopped accepting public donations to WikiLeaks and closed its account.[2] In December of that year, PayPal did the same,

1. Taylor Barnes, *Pentagon Threatens to 'Compel' WikiLeaks to Hand over Afghan War Data*, CHRISTIAN SCI. MONITOR (Aug. 6, 2010), http://www.csmonitor.com/World/terrorism-security/2010/0806/Pentagon-threatens-to-compel-WikiLeaks-to-hand-over-Afghan-war-data.

2. David Leigh & Rob Evans, *WikiLeaks Says Funding Has Been Blocked After Government Blacklisting*, THE GUARDIAN (Oct. 14, 2010, 12:55 AM), http://www.theguardian.com/media/2010/ oct/14/ wikileaks-says-funding-is-blocked; *About Us: Our Company*, SKRILL, https://www.skrill. com/en/about-us/ our-company/ (last visited July 5, 2015) (noting the rebrand of Moneybookers to Skrill in 2013).

followed shortly thereafter by Visa and MasterCard.[3] Cumulatively, these actions created a payment blockade that seriously threatened the site's continued existence. According to Assange, the blockade cost WikiLeaks 95% of its revenue and very nearly starved it to death.[4] None of the participating payment processors was under court order to block payments to WikiLeaks, and there had been no legal process in either the United Kingdom or the United States finding Assange or WikiLeaks guilty of any crime.[5] The blockade resulted from a series of business decisions by corporate executives and their risk managers. When queried by a journalist from *Forbes* about the reason for their actions, MasterCard and Visa offered no comment.[6] Moneybookers cited the fact that the U.S. government had added WikiLeaks to its "terrorism watchlist."[7] Documents later obtained and released by WikiLeaks in connection with a European Commission investigation of the blockade established that staffers for U.S. lawmakers directly pressured MasterCard and Visa to take the action they took.[8]

The crippling multilateral payment blockade to which WikiLeaks became subject highlights the existential power of payment intermediaries in the Internet ecosystem and the indirect control they can exercise over online transactions and associated speech. Whereas it is trivially easy for the operator of a seized or blacklisted domain name to relocate objectionable content to another domain, it is much more difficult for a website operator to replace a canceled banking relationship.[9] Indeed, payment intermediaries are uniquely positioned to

3. Andy Greenberg, *Visa, MasterCard Move to Choke WikiLeaks*, FORBES (Dec. 7, 2010, 10:16 AM), http://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/.

4. Esther Addley & Jason Deans, *WikiLeaks Suspends Publishing to Fight Financial Blockade*, THE GUARDIAN (Oct. 24, 2011, 8:42 AM), http://www.theguardian.com/media/2011/oct/24/wikileaks-suspends-publishing.

5. Glenn Greenwald, *Prosecution of Anonymous Activists Highlights War for Internet Control*, THE GUARDIAN (Nov. 23, 2012, 8:53 AM), http://www.theguardian.com/commentisfree/2012/nov/23/anonymous-trial-wikileaks-internet-freedom.

6. Greenberg, *supra* note 3.

7. Leigh & Evans, *supra* note 2.

8. *See* Press Ass'n, *Julian Assange Expresses Surprise over EU WikiLeaks Decision*, THE GUARDIAN (Nov. 27, 2012, 10:02 AM), http://www.theguardian.com/media/2012/nov/27/julian-assange-eu-wikileaks-decision; Greenwald, *supra* note 5 (reporting that Senate Homeland Security Committee Chairman Joe Lieberman was one of the sources of the pressure against WikiLeaks).

9. Damon McCoy et al., *Priceless: The Role of Payments in Abuse-advertised Goods*, 2012 ASS'N FOR COMPUTING MACHINERY CONF. ON COMPUTER & COMM. SECURITY 845, 847, *available at* http://dl.acm.org/citation.cfm?id=2382285 ("[A] miscreant can replace a suspended domain name within minutes at a cost of a few dollars, but if a banking relationship is shuttered they may lose hundreds of thousands of dollars in holdback and spend weeks developing a suitable

police online activity because approximately eighty percent of online transactions use a credit or debit card as a method of payment, and most of those transactions go through one of two payment systems: MasterCard or Visa.[10] As Ronald Mann and Seth Belzley have observed, concentration and high barriers to entry in the market for payment processing make payment intermediaries a logical choke point for regulators to target.[11] Moreover, payment blockades can reach online enterprises hosted abroad, thereby extending the reach of U.S. power and law beyond their territorial limits.[12]

Julian Assange managed to elude U.S. authorities by hiding out in the Ecuadorian embassy in London.[13] WikiLeaks was not so lucky, insofar as it was operationally reliant on private actors amenable to official pressure and well-situated to punish officially disapproved conduct.[14] The WikiLeaks payment blockade was an expression through private actors of the government's desire to regulate the flow of information over the Internet for law enforcement purposes. It serves as a fairly dramatic example of the ease with which the government can convince powerful corporate actors to do its bidding when behind-the-scenes pressure is brought to bear.[15] Public–private regulatory cooperation of this sort goes by many names in the First Amendment literature, including proxy

---

replacement."); *see also* Annemarie Bridy, *Carpe Omnia: Civil Forfeiture in the War on Drugs and the War on Piracy*, 46 ARIZ. ST. L.J. 683, 716–17 (2014) [hereinafter Bridy, *Carpe Omnia*] (explaining why domain name seizures have only transitory deterrent effects for online copyright enforcement).

10. Ronald J. Mann & Seth R. Belzley, *The Promise of Intermediary Liability*, 47 WM. & MARY L. REV. 239, 280 (2005).

11. *Id.* at 257–58; *see also* McCoy et al., *supra* note 9, at 847, § 2.3 ("Concentration, in addition to the small number of acquirers accepting high-risk merchants, the long setup time for new banking relationships, and the liability on revenue holdback, makes the payment tier an attractive target for those seeking to combat [online counterfeiting].").

12. *See* Mann & Belzley, *supra* note 10, at 279–80.

13. Scott Shane, *Offering Snowden Aid, WikiLeaks Gets Back in the Game*, N.Y. TIMES (June 23, 2013), http://www.nytimes.com/2013/06/24/world/offering-snowden-aid-wikileaks-gets-back-in-the-game.html.

14. *See* Press Ass'n, *supra* note 8.

15. The U.S. government successfully pressured other intermediaries to punish WikiLeaks as well. Amazon.com terminated hosting services for WikiLeaks' documents without any legal process or court order. Doug Gross, *WikiLeaks Cut off from Amazon Servers*, CNN (Dec. 2, 2010, 8:49 AM), http://edition.cnn.com/2010/US/12/01/wikileaks.amazon/index.html (reporting on the service termination and quoting Senator Lieberman's statement that Amazon had made the "right decision").

censorship,[16] soft censorship,[17] and "new-school" speech regulation.[18]

The U.S. government's approach to enlisting payment intermediaries as online law enforcers has historically been bimodal—a combination of straightforward command-and-control regulation, as seen in the online gambling context,[19] and less transparent behind-the-scenes pressure, as seen in the WikiLeaks case. The latter mode has been de rigueur in the areas of anti-counterfeiting and anti-piracy since the White House Office of the Intellectual Property Enforcement Coordinator (IPEC) came into existence in 2009.[20]

With the possibility of command-and-control regulation in the background—and sometimes with such regulation pending in Congress—IPEC has pressured a wide range of online intermediaries into adopting "voluntary best practices" for assisting in the enforcement of intellectual property rights.[21] The most visible voluntary agreement in

16. Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 14 (2006) ("The Internet's resistance to direct regulation of speakers and listeners rests on a complex chain of connections, and emerging regulatory mechanisms have begun to focus on the weak links in that chain. Rather than attacking speakers or listeners directly, governments have sought to enlist private actors within the chain as proxy censors to control the flow of information.").

17. Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 870 (2012) (contrasting "hard censorship" with "soft censorship" and including in the latter category "persuasion through pressure").

18. Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2298 (2014) (explaining that "new-school" techniques of speech regulation "regulate speech through control over digital networks and auxiliary services like search engines, payment systems, and advertisers; instead of focusing directly on publishers and speakers, they are aimed at the owners of digital infrastructure").

19. An example of command-and-control deputization of payment intermediaries as law enforcers is the Unlawful Internet Gaming Enforcement Act of 2006, 31 U.S.C. §§ 5361–5367 (2012), for which implementing regulations require financial institutions to identify and block illegal online gambling transactions. *See* Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L.J. 1037, 1065 & n.121 (2010).

20. *See, e.g.*, *Oversight of Intellectual Property Law Enforcement Efforts: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 4–5 (2011) (statement of Victoria A. Espinel, Intellectual Property Enforcement Coordinator, Office of Management and Budget), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg92565/pdf/CHRG-112shrg92565.pdf ("In addition to increased law enforcement against private infringement, we need cooperation and action from the private sector. . . . [W]e have been encouraging cooperative voluntary practices to reduce infringement online that are practical and effective . . . . We strongly support these voluntary agreements to help address counterfeiting and piracy online.").

21. *See, e.g.*, 2011 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT 1 (2012) [hereinafter 2011 IPEC REP.], *available at* https://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_mar2012.pdf (reporting on the adoption of best practices agreements by payment systems and Internet service providers); Victoria Espinel, *Coming Together to Combat Online Piracy and*

this space is the 2011 Memorandum of Understanding (MOU) between corporate copyright owners and residential broadband providers that created the Copyright Alert System (CAS), a graduated response protocol for mitigating infringement over peer-to-peer (P2P) file-sharing networks.[22] A lesser-known agreement was concluded in the same year by major payment processors and corporate copyright and trademark owners. That agreement, which established a notice-and-termination protocol for online merchants accused of piracy or counterfeiting, is the subject of this Article. The payment processors' best practices agreement serves as one more example of a mode of regulation that Julia Black has called "coerced self-regulation"[23] and that I have described elsewhere as state-promoted private ordering.[24] As Mann and Belzley put it, Internet intermediaries tend to coalesce around voluntary enforcement agreements "not in the shadow of existing law, but in the shadow of potential law."[25]

This Article addresses the use and efficacy of Internet payment blockades, or "follow the money" enforcement, for anti-counterfeiting and anti-piracy purposes. It focuses on the voluntary best practices

---

Counterfeiting, WHITEHOUSE.GOV (July 15, 2013, 8:33 AM), https://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting (reporting on the adoption of a best practices agreement by online advertising networks).

22. *See generally* Annemarie Bridy, *Graduated Response American Style: "Six Strikes" Measured Against Five Norms*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1 (2012) [hereinafter Bridy, *Graduated Response*] (assessing the CAS with respect to freedom of expression, privacy, fairness, proportionality, and transparency); Mary LaFrance, *Graduated Response by Industry Compact: Piercing the Black Box*, 30 CARDOZO ARTS & ENT. L.J. 165 (2012) (exploring problems relating to the MOU); Peter Yu, *The Graduated Response*, 62 FLA. L. REV. 1373 (2010) (discussing graduated responses generally).

23. Julia Black, *Constitutionalising Self-Regulation*, 59 MODERN L. REV. 24, 27 (1996). Black identifies four self-regulatory modes, each of which is defined in terms of the government's role in its development, adoption, and enforcement:

> Broadly, we can identify four types of possible relationship: *mandated* self-regulation, in which a collective group, an industry or profession for example, is required or designated by the government to formulate and enforce norms within a framework defined by the government, usually in broad terms; *sanctioned* self-regulation, in which the collective group itself formulates the regulation, which is then subjected to government approval; *coerced* self-regulation, in which the industry itself formulates and imposes regulation but in response to threats by the government that if it does not the government will impose statutory regulation; and *voluntary* self-regulation, where there is no active state involvement, direct or indirect, in promoting or mandating self-regulation.

Id. (footnotes omitted).

24. Annemarie Bridy, *ACTA and the Specter of Graduated Response*, 26 AM. U. INT'L L. REV. 559, 578 (2011).

25. Mann & Belzley, *supra* note 10, at 260 n.59.

agreement adopted in 2011 by payment processors, including American Express, Discover, MasterCard, PayPal, and Visa.[26] Part I discusses the regulatory environment that gave rise to the agreement. Part II describes the agreement itself, including the merchant termination protocol it specifies and the implementation of that protocol. Part III explores some normative concerns associated with the use of payment blockades as an anti-piracy and anti-counterfeiting strategy. Part IV considers the efficacy of payment blockades, taking into account methods of circumvention such as vouchers and virtual currencies.

I. WORKING TOWARD PAYMENT BLOCKADES: THE ROAD TO VOLUNTARISM

This Part surveys the copyright and trademark industries' multifaceted strategy for deputizing payment intermediaries in the fight against online counterfeiting and piracy. It traces industry efforts from the federal courts to Congress and, finally, to the executive branch, where IPEC put the weight of the White House behind a voluntary enforcement agreement that all major processors of online payments ultimately adopted.

A. *In the Courts: Perfect 10 and the Secondary Liability Gambit*

The road to voluntary payment blockades for anti-piracy and anti-counterfeiting enforcement begins with Perfect 10, a magazine publisher and website operator selling subscription-based access to "tasteful copyrighted images of the world's most beautiful natural models."[27] In 2004, Perfect 10 sued Visa, MasterCard, and other payment intermediaries (collectively, Visa) on the theory that they were contributorily and vicariously liable for infringements occurring on so-called Stolen Content Websites to which Visa provided payment processing services.[28] Perfect 10's secondary liability claims sounded in both copyright and trademark law.[29] The complaint alleged that Perfect 10 sent notices to Visa identifying the accused websites and stating that customers of those websites were using Visa cards to purchase infringing photographs.[30] Visa admitted to receiving the notices but took no action in response to them.[31] The district court dismissed the claims against Visa with prejudice on a Rule 12(b)(6) motion.[32] Perfect 10 appealed the

26. 2011 IPEC REP., *supra* note 21, at 1.

27. Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 793 (9th Cir. 2007) (internal quotation marks omitted).

28. *Id.* at 793, 805 n.18.

29. *Id.* at 793.

30. *Id.*

31. *Id.*

32. *Id.*

judgment to the U.S. Court of Appeals for the Ninth Circuit, which affirmed the dismissal over a lengthy and vehement dissent from Judge Alex Kozinski.[33]

A short primer on secondary liability doctrines in copyright and trademark law is helpful for understanding the challenge courts face in applying the doctrines to such functionally diverse online intermediaries as broadband access providers, payment processors, search engines, ad networks, auction platforms, and user-generated content sites. These doctrines are the primary legal mechanism for incentivizing online intermediaries to become regulators of their users' speech and activity.[34] No statutory cause of action exists for secondary infringement in either the Copyright Act or the Lanham Act, but the doctrines of contributory and vicarious infringement are well-established in both bodies of case law.[35] Trademark law, however, defines secondary infringement more narrowly than copyright law does.[36]

From a policy perspective, well-defined and carefully circumscribed secondary liability rules are necessary to prevent the injustice that could easily result from making one party pay for another's bad acts.[37] The common law standards for secondary infringement have evolved accordingly: where the allegation is of contributory infringement, the plaintiff must prove that the alleged secondary infringer acted culpably to facilitate the infringement; where the allegation is of vicarious infringement, the plaintiff must prove that the alleged secondary infringer's relationship to the direct infringer entailed a degree of control

33. *Id.* at 793; *id.* at 810 (Kozinski, J., dissenting).

34. *See* John Blevins, *Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms*, 34 CARDOZO L. REV. 1821, 1871–72 (2013).

35. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 434–35 (1984) ("The Copyright Act does not expressly render anyone liable for infringement committed by another. . . . The absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity."); Rosetta Stone Ltd. v. Google, Inc., 676 F.3d 144, 165 (4th Cir. 2012) ("Vicarious liability in the trademark context is essentially the same as in the tort context." (internal quotation marks omitted)); Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 103 (2d Cir. 2010) ("Contributory trademark infringement is a judicially created doctrine that derives from the common law of torts.").

36. Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1150 (7th Cir. 1992) (citing *Sony*, 464 U.S. at 439 n.19) (noting that there are "fundamental differences" between copyright law and trademark law for purposes of determining secondary liability).

37. *See Sony*, 464 U.S. at 435 (acknowledging that secondary infringement liability presents the "problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another").

that would justify holding the secondary infringer responsible for the wrongs of the direct infringer.[38]

1. Contributory Copyright Infringement

An online intermediary can be liable for contributory copyright infringement if it knows of its users' infringing activity and "induces, causes or materially contributes to [that] infringing conduct."[39] The requisite knowledge on the part of the accused can be actual or constructive, but in either case it must be knowledge of specific instances of infringing activity, as opposed to a generalized knowledge that direct infringement is occurring on the service in question.[40] Willful blindness to specific instances of infringement also constitutes knowledge, though the courts have not established the precise contours of the willful blindness doctrine in copyright cases.[41] To prove willful blindness, a plaintiff must show that the accused secondary infringer engaged in a "deliberate effort to avoid guilty knowledge."[42]

If a defendant "actively strives to provide the environment and the market for counterfeit . . . sales," then supplying the "site and facilities" for infringing activity is sufficient to establish the element of causation or material contribution.[43] Inducing direct infringement likewise entails active conduct intended to encourage direct infringement, such as advertising an infringing use of a product or service or instructing users how to use a product or service to infringe.[44] Some courts treat inducement as a distinct theory of secondary liability, but others treat it as a species of contributory infringement.[45] Courts have found inducement and material contribution separately where online service

38. *See* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1175 (9th Cir. 2007) (explaining that "in general, contributory liability is based on the defendant's failure to stop its own actions which facilitate third-party infringement, while vicarious liability is based on the defendant's failure to cause a third party to stop its directly infringing activities").

39. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019 (9th Cir. 2001) (quoting Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

40. *See id.* at 1021 (holding that "absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material").

41. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2d Cir. 2012); *In re* Aimster Copyright Litig., 334 F.3d 643, 650 (7th Cir. 2003).

42. *In re Aimster*, 334 F.3d at 650.

43. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1032 (9th Cir. 2013) (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996)).

44. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 936 (2005).

45. *Compare, e.g.*, Arista Records LLC v. Lime Grp. LLC, 784 F. Supp. 2d 398, 424 (S.D.N.Y. 2011) ("In *Grokster*, the Supreme Court confirmed that inducement of copyright infringement constitutes a distinct cause of action."), *with* Flava Works, Inc. v. Gunter, 689 F.3d 754, 758 (7th Cir. 2012) (describing inducement as "a form of contributory infringement").

providers help users to locate infringing files for download on the Internet.[46] At a more general level, courts have found inducement where a service provider "knowingly takes steps that are substantially certain to result in direct infringement."[47] This more general proposition highlights the role of causation in the contributory infringement analysis and the debt that secondary liability doctrines in copyright law owe to tort law.[48]

Evaluating Perfect 10's contributory infringement claim required the Ninth Circuit to decide how its prior decisions interpreting the "site and facilities" doctrine apply in an e-commerce context, where the defendant's services made direct infringement more profitable but were not otherwise implicated in it.[49] The majority adopted a carefully cabined interpretation of what it means to provide the "site and facilities" for infringement, reasoning that a broader interpretation would improvidently expand the scope of secondary liability to reach intermediaries whose systems are only peripherally related to infringing activities.[50] Although the majority acknowledged that Visa's payment systems "make it easier for . . . infringement to be profitable," it held that because the payment processors themselves were not essential to the conduct of directly infringing activities (i.e. reproduction, distribution, and public display), they made no material contribution to those activities.[51]

The majority differentiated payment systems like Visa's from the brick-and-mortar swap meet in *Fonovisa v. Cherry Auction*, pointing out that the infringing material in *Fonovisa* was "physically located in and

46. *See, e.g.*, Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1046 (9th Cir. 2013) (holding that there was inducement in a case involving the operator of a torrent tracker); Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007) (holding that there was material contribution in a case involving a search engine operator).

47. *Amazon.com*, 508 F.3d at 1171.

48. *See, e.g.*, Mark Bartholomew & Patrick F. McArdle, *Causing Infringement*, 64 VAND. L. REV. 675, 680 (2011). Mark Bartholomew and Patrick McArdle argue that tort law's concept of causation can potentially be useful to courts deciding contributory infringement claims because "[b]y tethering liability for the infringing acts of another to causation, courts can offer an explanation of contributory infringement liability that more closely maps onto social expectations of fairness and blame." *Id.* at 699. The professors also point out, however, that there is significant confusion in the copyright case law concerning the relationship between tort law principles of causation and the element of material contribution. *See id.* at 704–05 (arguing that "the causal analysis usually becomes confused with other issues of responsibility so that it is often impossible to determine what causal tests were actually used").

49. *See* Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788, 798–800 (9th Cir. 2007).

50. *See id.* at 800 (stating that "[a]ny conception of 'site and facilities' that encompasses Defendants would also include a number of peripherally-involved third parties, such as computer display companies, storage device companies, and software companies").

51. *Id.* at 794 n.1, 797–98.

traded at [Cherry Auction's] market."[52] The majority also differentiated cyberspace "sites" of infringement from Visa's payment system, explaining that the P2P file sharing system in *A&M Records v. Napster* provided "a centralized place . . . where infringing works could be collected, sorted, found, and bought, sold, or exchanged."[53] Visa, the majority said, "[does] not provide users the tools to locate infringing material, nor does any infringing material ever reside on or pass through any network or computer [Visa] operate[s]."[54] By this logic, Visa's payment system is not the "site" of any infringing activity; rather, the websites for which Visa's system processed payments are the "sites" of actual infringing activity.[55] On the issue of inducement, the majority held that Visa in no way designed or promoted its payment system as a means to infringe copyrights.[56] The majority concluded that having "the power to undermine the commercial viability of infringement" does not constitute material contribution to infringement or inducement to infringe.[57]

2. Contributory Trademark Infringement

An intermediary can be liable for contributory trademark infringement if it "intentionally induced" an underlying direct infringement or "continued to supply" either a service or an infringing product to a direct infringer while knowing of the direct infringement.[58] When the intermediary in question is a service provider rather than a product supplier, the service provider must exhibit "direct control and monitoring of the instrumentality" used by the direct infringer to infringe the mark.[59] These are higher hurdles for a plaintiff than the knowledge and material contribution standards in copyright law.[60]

Having already concluded that Visa was not liable for contributory copyright infringement, the majority easily concluded that Perfect 10 failed to carry its burden with respect to the more rigorous standards of trademark law.[61] Specifically, Perfect 10 alleged no affirmative acts by

52. *Id.* at 796.

53. *Id.* at 799.

54. *Id.* at 800.

55. *Id.* at 799.

56. *See id.* at 801 (citing Metro-Goldwyn-Meyer Studios Inc. v. Grokster, 545 U.S. 913, 925–26 (2005)) (observing that marketing credit cards as a means to pay for goods does not equate with marketing any specific goods for which people might pay using those credit cards).

57. *Id.* at 800–02.

58. *Id.* at 807 (internal quotation marks omitted).

59. *Id.*

60. *Id.* at 806 (citing Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 265 (9th Cir. 1996)) ("The tests for secondary trademark infringement are even more difficult to satisfy than those required to find secondary copyright infringement.").

61. *Id.*

Visa to support a claim that Visa induced its customers to infringe Perfect 10's marks.[62] Moreover, the majority said, echoing its reasoning concerning what constitutes a "site" of copyright infringement, Visa's payment network is not the "instrumentality" through which third parties infringe Perfect 10's trademarks.[63] The acts of direct infringement alleged by Perfect 10 occurred on third-party websites whose contents were beyond Visa's direct control as a payment processor.[64] Those sites, and not Visa's payment network, were the instrumentalities of direct infringement. At best, Visa could only indirectly control conduct on the sites where the primary infringements were occurring,[65] and indirect control cannot support a finding of liability.

3. Vicarious Copyright Infringement

Turning to vicarious copyright infringement, an online intermediary can be liable if it had, but declined to exercise, the right and ability to control or supervise a direct infringer from whose actions it directly profited.[66] The control element of a claim for vicarious copyright infringement requires both proof that the defendant had the legal right to control the actions of the direct infringer and proof that the defendant had the practical ability to do so.[67] That element is satisfied, for example, if the defendant reserves the right in its terms of service to terminate access for infringing users, and the architecture of the defendant's system enables the defendant to locate infringing material.[68] There is no scienter element to a claim of vicarious infringement, which is consonant with the agency law origins of the cause of action.[69] It doesn't matter whether the defendant *knew* what the direct infringer was doing; it matters only whether the defendant was in a position to *control* what the direct infringer was doing. The direct profit or financial benefit element is satisfied if infringing material is a draw for users or increases the attractiveness of the defendant's venue or service.[70] No actual pecuniary

62. *Id.* at 807.

63. *Id.*

64. *Id.*

65. *See id.*

66. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 & n.9 (2005).

67. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1173 (9th Cir. 2007) (citing *Grokster*, 545 U.S. at 930 n.9).

68. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023–24 (9th Cir. 2001).

69. *See Grokster*, 545 U.S. at 930 n.9, 932 (stating that "a vicarious liability theory . . . allows imposition of liability . . . even if the defendant initially lacks knowledge of the infringement").

70. *Napster*, 239 F.3d at 1023 (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263–64 (9th Cir. 1996)).

benefit (e.g., a commission on the sale of infringing works) is required.[71]

To evaluate Perfect 10's claim for vicarious infringement, the court had to consider whether the control element is satisfied when a payment processor has the right and ability to terminate payments to a site on which direct infringement is occurring, but has no direct control over the infringing content on the site. Perfect 10 argued that Visa's terms of service, which permit it to require member merchants to stop illegal activity as a condition of their continued receipt of payments, were sufficient to establish that the payment processor has the right and ability to control the content on member merchants' sites.[72] The majority disagreed, drawing a fine line between the ability to exert financial pressure on a merchant to induce it to alter its conduct and the right and ability to directly control the merchant's infringing conduct, which was the reproduction, alteration, and distribution of Perfect 10's copyrighted photographs.[73] The dispositive difference, the majority asserted, is between a payment processor's ability to *affect* infringement on third-party sites, which it can do, and its ability to actually *supervise and control* infringing acts on those sites, which it can't: "Defendants cannot take away the software the offending sites use to copy, alter, and distribute the infringing images, cannot remove those websites from the Internet, and cannot themselves block the distribution of those images over the Internet."[74] *Fonovisa* and *Napster*, the majority explained, did not support Perfect 10's argument because in both of those cases the defendants "had the right to remove individual infringers from the very place the infringement was happening."[75] The fact that infringements occur on Visa's merchants' websites instead of on Visa's payment system was central to the majority's reasoning concerning the control element, as it had been in the analysis of the site and facilities element of contributory infringement.

4. Vicarious Trademark Infringement

As with standards for contributory infringement, standards for vicarious infringement differ between copyright and trademark law. For an intermediary to be vicariously liable for trademark infringement, it must have acted in apparent or actual partnership with the direct infringer, and the two must "have authority to bind [each] other in transactions with third parties or exercise joint ownership or control over the infringing

71. *Fonovisa*, 76 F.3d at 263.
72. Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788, 804 (9th Cir. 2007).
73. *Id.* at 804–05.
74. *Id.* at 805.
75. *Id.*

product" or service.[76]

For the same reasons that the majority rejected Perfect 10's claim that Visa had the "right and ability to control" direct copyright infringements occurring on the accused websites, it rejected the claim that Visa and the operators of the accused websites exercised joint ownership or control over the direct trademark infringements.[77] In response to Perfect 10's allegation that Visa and the website operators were in a "symbiotic financial partnership," the majority pointed out that Visa did not share in the profits of infringement.[78] Rather, Visa simply processed payments and collected standard processing fees for each transaction.[79]

5. Judge Kozinski's Dissent

Dissenting with his typical acidity, Judge Kozinski accused the majority of "slam[ming] the courthouse door in [Perfect 10's] face."[80] He found it obvious that "knowingly provid[ing] a financial bridge between buyers and sellers of pirated works" gives rise to secondary copyright liability, both contributory and vicarious.[81] On the element of material contribution, he was dismissive of the majority's attempt to distinguish payment processors from search engine operators, which he pointed out can be held contributorily liable under the court's previous decision in *Amazon.com*.[82] The majority distinguished payment processors from search engine operators on the rationale that the latter, as information location tools, are more essential to infringement.[83] But search engine operators, Judge Kozinski countered, are no more essential than payment processors to the commission of infringing acts.[84] The two types of intermediaries, he said, are fungible when it comes to the importance of their roles in facilitating direct infringements.[85] Just as search engines play a substantial role in helping users locate infringing material, payment processors play a substantial role in helping users buy infringing

76. *Id.* at 807.

77. *Id.* at 808.

78. *Id.* at 807–08.

79. *Id.* at 808.

80. *Id.* at 810 (Kozinski, J., dissenting).

81. *Id.* at 810–11.

82. *Id.* at 811 (emphasis added) (internal quotation marks omitted).

83. *Id.* at 797–98 n.8 (majority opinion) ("Because location services lead Internet users directly to infringing images and often display them on the website of the service itself, we find that location services are more important and more essential—indeed, more 'material'—to infringement than payment services are.").

84. *See id.* at 811 (Kozinski, J., dissenting).

85. *See id.* ("If a consumer wishes to buy an infringing image from one of the Stolen Content Websites, he can do so by using Visa or MasterCard, just as he can use Google to find the infringing images in the first place.").

material: "It's not possible to distribute by sale without receiving compensation, so payment is in fact part of the infringement process."[86] He concluded that processing payment for infringing images "is not just an economic incentive for infringement; it's an essential step in the infringement process."[87] Thus, because payment processors are central to infringement, holding them liable would not risk sliding down a slippery slope that leads to liability for peripheral intermediaries.[88]

On the question of right and ability to control, Judge Kozinski agreed with Perfect 10 that Visa's terms of service give it both the contractual right to require merchants to cease illegal activities on their sites and the practical ability to do so.[89] By his reasoning, control of the mechanics of transferring infringing material is not necessary to satisfy the control element because payment and distribution are inextricably linked: "In a commercial environment, distribution and payment are (to use a quaint anachronism) like love and marriage—you can't have one without the other. If cards don't process payment, pirates don't deliver booty."[90] Moreover, he said, if the ability to control is understood as the court defined it in *Amazon.com*—not just the ability to stop infringement but also the ability to limit it—then payment processors have that ability because withdrawing financial support from a website threatens its continued viability even if the site can survive.[91] Judge Kozinski accused the majority of substituting the "practical ability" test from *Amazon.com* for an "absolute right to stop" standard.[92] He saw no principled way, following the court's decision in *Amazon.com*, to let payment processors off the hook for failing to exercise their contractual right to require merchants to stop directly infringing.[93]

With respect to Visa's secondary liability under trademark law, Judge Kozinski was no less scathing in his criticism of the majority's reasoning

86. *Id.* at 814.

87. *Id.* at 812.

88. *See id.* at 816 ("Were we to rule for plaintiff, as we should, I have every confidence that future courts would be able to distinguish this case when and if they are confronted with lawsuits against utility companies, software vendors and others who provide incidental services to infringers.").

89. *Id.* at 816–17 ("[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.").

90. *Id.* at 818.

91. *See id.* at 818–19 (emphasizing that "[t]he standard is 'stop *or limit*' the infringing conduct" and positing that the difficulty of receiving payment for selling unlawful products will dramatically affect a website's operations).

92. *Id.* at 818.

93. *See id.*

and conclusions.[94] He found the requisite "control and monitoring" elements to support Perfect 10's claim of contributory infringement in Visa's ability to approve or deny the processing of any given payment.[95] And whereas the majority saw no "symbiotic partnership" between Visa and the operators of the accused websites for purposes of establishing vicarious liability,[96] Judge Kozinski asserted that payment processors like Visa reap "huge profits" from processing payments for infringing and counterfeit goods.[97] "If this is not symbiosis," he asked, "what is?"[98]

6. Making Sense of the Split Decision

The majority and the dissent in *Visa* are painstakingly reasoned, minutely responsive to each other, and about as diametrically opposed as two lines of reasoning on the same issues can possibly be. For as plausible as Judge Kozinski's dissent was, and for as strained as the majority's efforts were to avoid *Amazon.com* by distinguishing search engine operators from payment processors, the majority's decision is both legible and defensible as a matter of fairness and innovation policy.[99]

The majority declined to subject Visa and its co-defendants to liability for secondary copyright infringements from which they could not have insulated themselves by complying with the safe harbor provisions in the Digital Millennium Copyright Act (DMCA).[100] Although Congress drafted the DMCA's safe harbors with the intention of letting the courts develop secondary liability doctrines for online intermediaries,[101] Congress also designed the safe harbors "to facilitate the robust development and world-wide expansion of electronic commerce."[102] The omission of payment processors, which are the lynchpin of e-commerce, from the DMCA's safe harbor framework suggests that Congress neither

94. *Id.* at 822.

95. *Id.*

96. *Id.* at 808 (majority opinion).

97. *Id.* at 822–23 (Kozinski, J., dissenting).

98. *Id.* at 823.

99. *Cf.* Bartholomew & McArdle, *supra* note 48, at 711 (referring to the majority's analysis as "tortured" and arguing that it would have been preferable for the majority to base its holding explicitly on policy considerations).

100. The DMCA's safe harbors cover online service providers engaged in specific activities that may implicate infringing materials: routing and transmission, system caching, storing material at the direction of users, and hypertext linking. *See* 17 U.S.C. § 512(a)–(d) (2012). Payment processing is not a covered activity. *See id.*

101. *See* S. REP. NO. 105-190, at 19 (1998) ("Rather than embarking upon a wholesale clarification of these doctrines, the Committee decided to leave current law in its evolving state and, instead, to create a series of 'safe harbors,' for certain common activities of service providers.").

102. *Id.* at 1.

contemplated nor foresaw that copyright's secondary liability doctrines could stretch far enough to encompass them.[103] It seems highly unlikely that Congress would have intentionally excluded payment processors from safe harbor, given their importance to the expansion of e-commerce. In *Amazon.com*, Google was able to assert the DMCA's section 512(d) safe harbor for information location tools.[104] In *Visa*, by contrast, the defendant payment processors could not have invoked any section 512 safe harbor, leaving them wide open to crippling statutory damages.[105] That fact made a difference to the majority, which was concerned that secondary liability for payment processors would have a chilling effect on e-commerce.[106] It made no difference whatsoever to Judge Kozinski, who viewed payment processors not as the engine of e-commerce but as "marauders who pilfer the property of law-abiding, tax-paying rights holders, and who turn consumers into recipients of stolen property."[107] He was equally unmoved by the prospect that ineligibility for safe harbor puts payment processors in an unfair bind.[108]

It is undoubtedly true, as Mark Bartholomew and Patrick McArdle have argued, that the split decision in *Visa* highlights the instability inherent in secondary infringement doctrines and the extent to which that instability predisposes secondary infringement analyses to

103. Payment processors were active online intermediaries at the time Congress was drafting the DMCA. Credit card payments were accepted on the Internet as early as 1994. *See* Jacqueline Day, *Internet Commerce Kicks Off*, BANK SYS. & TECH., Dec. 1994, at 12, 14. In 1996, there was a total of $347 million in credit card transactions on the Internet, and rapid growth in e-commerce was projected as security for online transactions improved, causing consumer confidence to increase. *See* John N. Frank, *In Quest of CyberGold*, CREDIT CARD MGMT., Aug. 1996, at 48.

104. *See* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1175 (9th Cir. 2007) ("Google claims that it qualifies for the limitations on liability set forth in . . . § 512. In particular, [§] 512(d) limits the liability of a service provider 'for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link' if the service provider meets certain criteria.").

105. *See* Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788, 796 n.4 (9th Cir. 2007) (noting that Perfect 10 sought the "anomalous result" of holding Visa liable for third-party infringements that it could not have protected itself from by claiming safe harbor, both because it was not an eligible "service provider" within the meaning of the DMCA and because it lacked the ability to remove infringing content from its merchants' sites).

106. *See id.* at 794 ("We evaluate Perfect 10's claims with an awareness that credit cards serve as the primary engine of electronic commerce and that Congress has determined it to be the policy of the United States . . . to promote the continued development of the Internet . . . ." (internal quotation marks omitted)).

107. *Id.* at 824 (Kozinski, J., dissenting).

108. *See id.* at 824 n.25 (asserting matter-of-factly that "there is no anomaly in treating parties that are covered by the statute differently from those that are not").

unacknowledged policy-driven rationales.[109] It is also true, however, that policy considerations have a legitimate role to play when claimants invite courts to expand existing common law liability doctrines beyond their recognized scope. As a practical matter, *Visa* marked the end of the road for rights owners' efforts to use secondary liability rules to compel payment processors to stop the flow of money to alleged "Stolen Content Websites." In 2008, the U.S. Supreme Court denied Perfect 10's petition for certiorari, letting the Ninth Circuit's judgment in favor of Visa stand.[110] No one has re-litigated the issue since, and rights owners strategically shifted their attention in the wake of *Visa* to other regulatory venues in pursuit of their "follow the money" enforcement agenda.

B. *In Congress: The Shadow of Potential Law*

Between 2010 and 2011, members of Congress introduced three bills containing provisions requiring payment processors and other online intermediaries to block so-called foreign infringing or rogue sites: the Combating Online Infringements and Counterfeits Act (COICA),[111] the Stop Online Piracy Act (SOPA),[112] and the Protect Intellectual Property Act (PIPA).[113] The sound recording and motion picture industries lobbied aggressively for all three.[114] COICA didn't get much attention beyond the Beltway, but SOPA and PIPA ignited a media firestorm and public outcry that will not soon be forgotten on Capitol Hill:

> Online opposition to the two bills coalesced quickly as word spread that SOPA/PIPA contained provisions requiring the blacklisting of websites. In an open letter to Congress,

---

109. *See* Bartholomew & McArdle, *supra* note 48, at 710–11 (arguing that the *Visa* majority should have "acknowledge[d] that the *Amazon.com* decision relied on public policy, not the 'materiality' of the search engine's conduct, and then explain[ed], again on public policy grounds, why online credit card services should not be part of the 'simple measures' rule for online contributory infringement").

110. Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 553 U.S. 1079 (2008).

111. Combating Online Infringements and Counterfeits Act (COICA), S. 3804, 111th Cong. (2010).

112. Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (1st Sess. 2011).

113. Protect Intellectual Property Act (PIPA), S. 968, 112th Cong. (2011).

114. *See, e.g.*, Ernesto Van der Sar, *MPAA/RIAA Lobbied Extensively in Favor of Domain Seizures*, TORRENTFREAK (Dec. 19, 2010), https://torrentfreak.com/mpaariaa-lobbied-extensively-in-favor-of-domain-seizures-101219/ (reporting that the Recording Industry Association of America and MPAA spent more than $1.8 million in the third quarter of 2010 on lobbying efforts directly targeted at COICA and related site-blocking enforcement measures); Daniel Nasaw, *Who Backs the Anti-Piracy Laws?*, BBC NEWS (Jan. 18, 2012), http://www.bbc.co.uk/news/mobile/world-us-canada-16603870 (reporting on support for SOPA and PIPA by "the largest film, television, music recording and book publishing companies and trade associations in the US").

> Google co-founder Sergey Brin and other prominent Internet entrepreneurs asserted that the legislation would give the U.S. government "power to censor the web using techniques similar to those used by China . . . and Iran." Contributing to and marshaling web-roots resistance, the operators of Wikipedia made the unprecedented decision to "go dark" in protest for one day—January 18, 2012. In addition to Wikipedia, more than 100,000 Internet companies, including Google, Mozilla, Reddit, and I Can Has Cheezburger (of LOLcats fame), joined the one-day protest. Their forms of protest varied, but their message to their users and fans was unitary: "Petition your elected representatives to oppose these bills." And petition their representatives people did—in droves. Google reported that 4.5 million people in one day signed its petition opposing SOPA and PIPA.[115]

The provisions in the bills that became lightning rods for criticism were those requiring domain name system (DNS) authorities in the United States to prevent domain names associated with "rogue sites" from resolving to their designated Internet Protocol (IP) addresses.[116] Network engineers predicted that government orders to U.S.-based DNS authorities to block certain websites would lead some of the more sophisticated parties hosting those sites to create splinter or parallel systems for resolving domain names, thus fragmenting the unified structure of the DNS, on which the integrity of the Internet's global addressing system depends.[117] Such fragmentation, the bills' opponents asserted, would effectively "break the Internet."[118]

The provisions impacting payment processors attracted little

---

115. Annemarie Bridy, *Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Perspective on ACTA, SOPA, and PIPA*, 30 CARDOZO ARTS & ENT. L.J. 153, 159 (2012) (footnotes omitted).

116. *See* COICA, S. 3804 § 2 (as introduced in the Senate); SOPA, H.R. 3261 § 102; PIPA, S. 968 § 3.

117. *See, e.g.*, Paul Vixie, *On Mandated Content Blocking in the Domain Name System*, CIRCLEID (Mar 18, 2011, 12:14 PM), http://www.circleid.com/posts/20110318_on_mandated_content_blocking_in_the_domain_name_system/ ("My greatest worry is what people will do to bypass all this junk or to prevent other people from bypassing it. My fellow humans are a proud and occasionally adversarial bunch and they don't like being told what they can't do or what they have to do. The things we'll all be doing to bypass the local DNS restrictions imposed by our coffee shops or our governments or our ISPs will break *everything*. Where this ends is with questions like 'which DNS system are you using?' and 'which DNS systems is your TLD in?' which in other words means that where this ends is a world without universal naming.").

118. *See, e.g.*, Mark Lemley, David S. Levine & David G. Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (2011) ("Directing the remedial power of the courts towards the Internet's core technical infrastructure in this sledgehammer fashion has impact far beyond intellectual property rights enforcement—it threatens the fundamental principle of interconnectivity that is at the very heart of the Internet.").

attention, but they were an integral part of the bills' comprehensive, multi-intermediary approach to eliminating targeted sites from the Internet.[119] The relevant provisions were virtually identical across the three pieces of legislation: COICA required "a financial transaction provider" to "take reasonable measures . . . to prevent . . . its service from processing transactions for customers located within the United States based on purchases associated with the domain name; and . . . its trademarks from being authorized for use on Internet sites associated with such domain name."[120] SOPA required "a payment network provider . . . [to] take technically feasible and reasonable measures . . . to prevent, prohibit, or suspend its service from completing payment transactions involving customers located within the United States . . . and the payment account . . . which is used by the foreign infringing site."[121] PIPA required "a financial transaction provider . . . [to] take reasonable measures . . . designed to prevent, prohibit, or suspend its service from completing payment transactions involving customers located within the United States and the Internet site associated with the [targeted] domain name."[122]

It is difficult to predict how COICA, SOPA, and PIPA would have fared had they not contained the controversial DNS provisions that ultimately doomed them. Responses to the legislation among the major payment processors were divided, with a majority opposed.[123] MasterCard's Head of Franchise Development and Customer Performance Integrity testified in favor of SOPA at the House Judiciary Committee hearing, stating for the record that "MasterCard ha[d] forged strong working relationships with rights holders and their trade associations" and was then "working with [IPEC] in the development of industry best practices to address copyright infringement and the sale of

119. Other intermediaries required to engage in blocking were search engine operators and online advertising networks. *See, e.g.*, SOPA, H.R. 3261 § 102 (prohibiting search engines from returning links to targeted sites in search results and advertising services from serving advertisements alongside the content on such sites).

120. COICA, S. 3804 § 2.

121. SOPA, H.R. 3261 § 102.

122. PIPA, S. 968, 112th Cong. § 3 (2011).

123. *See List of Supporters and Opponents of H.R. 3261*, OPENCONGRESS, http://www.opencongress.org/bill/hr3261-112/bill_positions (last visited July 5, 2015) (noting Visa's support for and PayPal's opposition to SOPA); *see also* Brett Greene, *SOPA and PIPA Bills Threaten Job Creation and Innovation*, HUFFINGTON POST (Jan. 13, 2012, 5:12 AM), https://secure.huffingtonpost.com/brett-greene/sopa-and-pipa-bills-threa_b_1204825.html (recognizing American Express, Discover, and PayPal's opposition to SOPA and PIPA); Connor Adams Sheets, *SOPA Supporters: Companies and Groups That Support the Controversial Bill*, INT'L BUS. TIMES (Jan. 5, 2012, 9:46 AM), http://www.ibtimes.com/sopa-supporters-companies-groups-support-controversial-bill-391250 (observing Visa and MasterCard's support for SOPA).

counterfeit products over the Internet."[124] Although MasterCard was the only payment processor to make a public statement to that effect, many others were then participating in a parallel executive-branch effort to secure their cooperation as copyright and trademark enforcers. That effort resulted in the voluntary best practices agreement discussed at length in Part II below. The document, dated May 16, 2011—more than five months before SOPA was introduced in the House of Representatives—carried the endorsement of five major payment processors.[125] To the extent that the threat of command-and-control intervention created a regulatory environment conducive to the conclusion of a more flexible, non-binding voluntary agreement—and it seems fair to infer that it did—that threat was embodied in COICA.

C. *In the White House: IPEC and the Paradox of Non-Regulatory Regulation*

IPEC has prodded all of the online intermediaries that would have been subject to the mandatory blocking provisions in COICA, SOPA, and PIPA—payment processors, search engines, domain name registry operators (i.e., Internet service providers), and online advertising networks—to implement equivalent blocking protocols through voluntary agreements. In its first Joint Strategic Plan (JSP), published in 2010, IPEC announced its intent to "encourage" private-sector cooperation to reduce online infringement and counterfeiting:

> The Administration encourages cooperative efforts within the business community to reduce Internet piracy. The Administration believes that it is essential for the private sector, including content owners, Internet service providers, advertising brokers, payment processors and search engines, to work collaboratively, consistent with the antitrust laws, to address activity that has a negative economic impact and undermines U.S. businesses, and to seek practical and efficient solutions to address infringement. This should be achieved through carefully crafted and balanced agreements.[126]

---

124. *Stop Online Piracy Act: Hearing Before the Comm. on the Judiciary H.R. on H.R. 3261*, 112th Cong. 82–83, 85 (2011) [hereinafter *SOPA Hearing*] (statement of Linda Kirkpatrick, Group Head, Customer Performance Integrity, MasterCard Worldwide).

125. *See* Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet (May 16, 2011) [hereinafter Best Practices for Payment Processors] (on file with author) (listing American Express, Discover, MasterCard, PayPal, and Visa as participating payment processors).

126. 2010 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 17 (2010) [hereinafter 2010 JSP], *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf.

The 2011 JSP recapitulated the theme of voluntary cooperation but asserted a more active, facilitative role for IPEC in the process:

> Since the release of the Strategy, we have facilitated and encouraged dialogue among the different private sector Internet intermediaries that contribute to the dynamic nature and functioning of the Internet, including payment processors, search engines, and domain name registrars and registries. These entities can support efforts by rightholders and law enforcement to reduce online infringement in a manner consistent with our commitment to the principles of fair process, freedom of expression and other important public policy objectives. We believe that most companies share the view that providing services to infringing sites is inconsistent with good corporate business practice, and we are beginning to see several companies take the lead in pursuing voluntary cooperative action.[127]

In 2012, IPEC was more specific about the nature of the cooperation it encouraged, cloaking references to website blocking—a four-letter word following the SOPA and PIPA debates—in the language of epidemiology and contagion control: "We have facilitated voluntary agreements to 'quarantine' sites engaged in counterfeiting and piracy by working cooperatively with credit card companies, domain name registrars, and online advertisers."[128]

In its 2013 JSP, IPEC boasted a number of successes in the realm of "facilitating" voluntary agreements, including the best practices agreement for payment processors, the creation of the Center for Safe Internet Pharmacies "to combat fake online 'pharmacies' selling dangerous illegal drugs over the Internet," the graduated response MOU between broadband providers and rights owners, and a "leadership pledge" by advertisers "to not support online piracy and counterfeiting with advertising revenue."[129] Coming quickly on the heels of the

127. 2011 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR JOINT STRATEGIC PLAN 5 (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_anniversary_report.pdf.

128. 2012 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR JOINT STRATEGIC PLAN ii (2012), *available at* https://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_two-year_anniversary_report.pdf.

129. 2013 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 1, 35–36 (2013) [hereinafter 2013 JSP], *available at* https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

leadership pledge by advertisers was a voluntary best practices agreement for advertising networks.[130]

The precise nature of IPEC's facilitation of voluntary agreements is unclear; however, the very fact that the government convenes and participates in negotiations over such agreements calls their voluntariness into question.[131] IPEC characterizes its approach to private-sector cooperation as a "voluntary, non-regulatory" one,[132] but that is an oversimplification. The approach is certainly non-regulatory in the literal sense: it has produced no new public laws, and there is no public record of IPEC's involvement in the negotiation of any of the voluntary agreements for which it has taken credit. It *is* regulatory, however, in the very real sense that the government is playing an active role in the formation of "sticky" (and sometimes legally binding) industrial norms. Julia Black's distinction between voluntary self-regulation and coerced self-regulation is fitting in this context.[133] IPEC regards "best practices" intellectual property enforcement agreements as a form of voluntary self-regulation, but calling an agreement voluntary doesn't make it so. If the administration's approach were truly non-regulatory, then IPEC would not act as a midwife to these agreements and publicly claim credit when they are born. Moreover, IPEC makes specific legislative recommendations in its annual JSPs, which means that the shadow of potential law hangs perennially over the private-sector conversations that it facilitates.[134] In light of these realities, it is more honest to classify voluntary agreements as a form of regulation by arm-twisting.[135]

Adding further to the regulatory ambiguity surrounding voluntary agreements, IPEC's 2013 JSP directed the U.S. Patent and Trademark

130. *See* Espinel, *supra* note 21 (announcing that "24/7 Media, Adtegrity, AOL, Condé Nast, Google, Microsoft, SpotXchange, and Yahoo!, with the support of the Interactive Advertising Bureau, committed to a set of best practices to address online infringement by reducing the flow of ad revenue to operators of [rogue] sites").

131. *See, e.g.*, 2013 JSP, *supra* note 129, at 35–36.

132. *Id.* at 36.

133. *See supra* text accompanying note 23 (explaining Black's regulatory taxonomy).

134. *See, e.g.*, 2010 JSP, *supra* note 126, at 22 (including a "Comprehensive Review of Existing Intellectual Property Laws to Determine Needed Legislative Changes" in a list of "Action Items"); ADMINISTRATION'S WHITE PAPER ON INTELL. PROP. ENFORCEMENT LEGIS. RECOMMENDATIONS 1–3 (2011), https://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf (recommending twenty-three changes to existing laws to enhance enforcement efforts).

135. *See* Ronald J. Mann, *Emerging Frameworks for Policing Internet Intermediaries*, 10 J. INTERNET L. 3, 8 (2006) ("In practice, regulators have become increasingly adept at securing voluntary agreements, apparently out of the payment intermediaries' desire to forestall more intrusive regulation.").

Office (USPTO) to conduct an official study to assess their efficacy.[136] Less than three months after that study began, the House Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet held a hearing on the same subject,[137] signaling coordination between the two branches and an official expectation, however vague, of measurable results. In his opening statement at the House hearing, Representative Mel Watt was candid about the causal relationship between threatened regulation and private-sector voluntarism: "We are certainly not here to relitigate SOPA," he said, "but I do believe that the SOPA debate . . . helped motivate an important shift in the willingness of some parties to engage more aggressively in negotiating . . . some of the best practices we are considering here today."[138] "Indeed," he continued, "some of the entities that fought vigorously to defeat SOPA are now constructive parties to voluntary agreements designed to combat the drain on our economy . . . that online piracy and counterfeiting represent."[139] As the Motion Picture Association of America (MPAA) acknowledged with equal candor in comments submitted for the USPTO study, "a party's willingness to commit to a particular practice will depend to a significant degree on what it perceives to be the legal consequence (or lack thereof) of continuing its current course of action, and not committing to any voluntary agreement."[140] The regulatory dynamic is implicit but clear: volunteer or be compelled.

When the government takes so active an interest in the negotiation and performance of private-sector agreements as it has taken in the online intellectual property enforcement space, the line between public and private law becomes blurred in ways that may ultimately undermine desired regulatory outcomes. In its comments for the USPTO study, the Computer & Communications Industry Association (CCIA) questioned both the basis for and the wisdom of de facto governmental oversight of private-sector agreements:

136. *See* Request of the United States Patent and Trademark Office (USPTO) for Public Comments: Voluntary Best Practices Study, 78 Fed. Reg. 37210 (June 20, 2013).

137. *Role of Voluntary Agreements in the U.S. Intellectual Property System: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the Comm. on the Judiciary H.R.*, 113th Cong. (2013) [hereinafter *Role of Voluntary Agreements*], *available at* http://judiciary.house.gov/ (search for 113-49).

138. *Id.* at 2 (statement of Rep. Mel Watt, Member, H. Comm. on the Judiciary).

139. *Id.*

140. Comments of the Motion Picture Association of America in Response to Request of the USPTO for Public Comments: Voluntary Best Practices Study 2 (Aug. 21, 2013), *available at* http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf.

> The [IPEC JSP] provided no indication of the basis for this directive; rather, it proceeded from the unexamined premise that the U.S. Government should be evaluating unregulated, private sector action in the first place. This proposal itself deserves additional consideration. Depending on the nature of the evaluation, industry stakeholders may perceive government assessments as a form of soft regulation. Should government evaluation be perceived as imposing regulatory compliance burdens, it will deter participation in "voluntary best practices," particularly if policymakers should characterize one given effort as superior to another, toward meeting some yet-unstated metric. Such evaluation may also be perceived as setting a minimum bar of regulatory compliance necessary for market entry.[141]

The CCIA's comments highlight the potentially distorting and counterproductive effects of coerced self-regulation on the affected actors and markets. If, as a regulatory reality, voluntary best practices agreements are voluntary in name only, Internet intermediaries may be willing to roll the dice on what the MPAA calls "improvements in the law,"[142] especially after the spectacular demise of SOPA and PIPA.

Despite IPEC's assertion that its approach to securing cooperation from online intermediaries is non-regulatory, the administration can't seem to decide if it is engaged in regulation or not when it "facilitates" the formation of voluntary agreements. In response to a Freedom of Information Act (FOIA) request for documents relating to the negotiation of the best practices agreement for payment processors, IPEC identified more than sixty responsive documents in its possession but declined to produce a single one, citing, *inter alia*, the deliberative process privilege in Exemption 5.[143] According to the U.S. Department of Justice, "the general purpose of [Exemption 5] is to prevent injury to the quality of agency decisions."[144] The cases establish two criteria, both of which must be met, for invoking the deliberative process privilege to deny a FOIA

---

141. Comments of the Computer & Communications Indus. Association in Response to Request of the USPTO for Public Comments: Voluntary Best Practices Study 1 (Aug. 21, 2013), *available at* http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf.

142. *See* Comments of the Motion Picture Association of America, *supra* note 140, at 3.

143. *See* Letter from Dionne Hardy, Office of Management & Budget, to Diana Gleason (Feb. 19, 2014) (on file with author) (stating that "[w]e are withholding . . . various drafts of such agreement and other related documents under FOIA Exemption 4 and FOIA Exemption 5. Exemption 5 protects interagency and intra-agency pre-decisional, deliberative materials, the disclosure of which would inhibit the frank and candid exchange of views that is necessary for effective government decision-making" (citation omitted)).

144. U.S. DEP'T OF JUSTICE, GUIDE TO THE FREEDOM OF INFORMATION ACT: EXEMPTION 5, at 13 (2009 ed.) (internal quotation marks omitted), *available at* http://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption5.pdf.

request: First, the requested document must be pre-decisional, meaning that it is "antecedent to the adoption of an agency policy."[145] Second, the document must be deliberative, meaning that it is "a direct part of the deliberative process in that it makes recommendations or expresses opinions on legal or policy matters."[146] For documents in IPEC's hands relating to the negotiation of the best practices agreement for payment processors, the first criterion is clearly not met because the documents are not antecedent to the adoption of any agency policy. IPEC's refusal to disclose the documents, however, amounts to an assertion that they *were* implicated in the formation of public policy.[147] And that assertion runs counter to IPEC's representation that its approach to securing intermediaries' cooperation is non-regulatory. The dissonance reflects the ambiguous status of IPEC-facilitated voluntary agreements and the need for the government to get its regulatory story straight vis-à-vis both the public and the intermediaries whose cooperation it seeks.

II. HOW PAYMENT BLOCKADES WORK: "BEST PRACTICES TO ADDRESS COPYRIGHT INFRINGEMENT AND THE SALE OF COUNTERFEIT PRODUCTS ON THE INTERNET"

The voluntary best practices agreement for payment processors is actually a two-sided proposition, insofar as it incorporates a complementary set of best practices for rights owners.[148] The participating payment processors named in the agreement are American Express, Discover, MasterCard, Visa, and PayPal.[149] There are no named rights owners in the agreement, but according to a report prepared for IPEC by the International AntiCounterfeiting Coalition (IACC), which administers the agreement, there are thirty-one participating rights owners, including manufacturers of apparel, shoes, luxury goods, electronics, cars, cigarettes, pharmaceuticals, software, and consumer products.[150] The two sets of best practices were adopted, respectively, in

145. Jordan v. U.S. Dep't of Justice, 591 F.2d 753, 774 (D.C. Cir. 1978) (en banc) (internal quotation marks omitted).

146. Vaughn v. Rosen, 523 F.2d 1136, 1143–44 (D.C. Cir. 1975).

147. After a lapse of time beyond what FOIA permits, multiple phone calls to the relevant FOIA officer, and additional written requests explaining why the asserted exemptions were inapplicable, IPEC eventually produced the responsive documents in its possession.

148. *See* Best Practices for Payment Processors, *supra* note 125; Best Practices for Rights-Holders with Payment Processors (July 2011) [hereinafter Best Practices for Rights-Holders] (on file with author).

149. Best Practices for Payment Processors, *supra* note 125, at 1.

150. *See* KRISTINA MONTANARO, INTL ANTICOUNTERFEITING COAL., EXECUTIVE SUMMARY: IACC PAYMENT PROCESSOR PORTAL PROGRAM: FIRST YEAR STATISTICAL REVIEW 3 (2012) [hereinafter EXECUTIVE SUMMARY], *available at* http://www.gacg.org/Content/Upload/

May and July 2011.[151] They were implemented in January 2012 with the launch of the Payment Processor Initiative, an inter-industry enforcement effort run by the IACC and marketed under the trademark "RogueBlock."[152] Following the program's initial implementation, the number of participating payment processors expanded to include PULSE and Diners Club.[153]

The IACC's role in administering the Payment Processor Initiative is roughly analogous to the role the Center for Copyright Information plays in administering the CAS.[154] Similar to the graduated response protocol in the CAS, to which broadband users become bound through terms of service with their providers, the enforcement protocol in the best practices agreement becomes binding on merchants through payment processors' policies, which prohibit the use of card services for illegal transactions.[155] There is, however, a very important difference between the voluntary best practices agreement for payment processors and the MOU that created the CAS: the best practices agreement is, by its express terms, not legally binding on the participating parties.[156] Although the terms of the agreement are sufficiently specific to be enforced, the parties disclaim contractual intent.

A. *The Protocol for Payment Processors*

At the core of the best practices agreement for payment processors is a notice-and-termination protocol. The protocol is operationalized through the RogueBlock "Portal Program," a web-based software system

---

MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf (describing the program).

151. Best Practices for Payment Processors, *supra* note 125, at 1; Best Practices for Rights-Holders, *supra* note 148, at 1.

152. *IACC Payment Processor Initiative (RogueBlock®)*, IACC, http://www.iacc.org/rogueblock.html (last visited July 5, 2015) [hereinafter *RogueBlock*] ("The initiative launched in January 2012, following rights-holder negotiations with the payment industry to develop a set of best practices in addressing rogue websites, as encouraged by the U.S. Intellectual Property Enforcement Coordinator, Victoria Espinel.").

153. *See Payment Processor Initiative & Portal Program: Innovation from Partnership*, IACC, [hereinafter *Payment Processor Initiative & Portal Program*], https://web.archive.org/web/20130119105913/http://c.ymcdn.com/sites/members.iacc.org/resource/resmgr/IACC_PaymentProcessorInitiat.pdf (last visited July 5, 2015) (listing participating payment processors).

154. *See* Bridy, *Graduated Response*, *supra* note 22, at 27–28 (explaining the role of the Center for Copyright Information).

155. *See* EXECUTIVE SUMMARY, *supra* note 150, at 3 ("The Portal Program is dependent on Card Network policies, which prohibit merchants from using card services for illegal transactions. Use of card services for sales of counterfeit or pirated goods constitutes a breach of these policies, and thus provides for remediation of the corresponding merchant account.").

156. *See* Best Practices for Payment Processors, *supra* note 125, at 4 ("These best practices are voluntary and not legally binding.").

for managing communications between rights owners and payment processors concerning alleged "rogue sites."[157] Rights owners pay annual fees for access to the program.[158] The program's front end is a secure online portal through which participating rights owners submit complaints containing information specified in the best practices agreement.[159] The portal provides a standardized, fillable web form for this purpose.[160] The program limits rights owners to "a maximum of twenty-five complaints per month."[161] On the back end of the program, the IACC reviews complaints and relays them to the relevant payment processor, which takes action as specified in the best practices agreement.[162] The payment processor then reports back to the IACC about the outcome of each complaint.[163] Rights owners can track the status of complaints and view outcomes via the online portal.[164]

A complaint from a rights owner under the agreement must contain four elements to be actionable: (1) a description of the alleged infringement and the "Illegitimate Products," including the identity of the website in question; (2) evidence that infringing products are available on the website using the payment processor's services (e.g., a screenshot of a payment processor's logo on the site); (3) a copy of a cease-and-desist letter or DMCA notice from the rights owner notifying the website's owner of the allegation of infringement, or an attestation that, to the best of the rights owner's knowledge, the site is not licensed or authorized to distribute the products; and (4) evidence that the requester owns the copyright or trademark in question.[165] If the payment processor requires additional information concerning the complaint, the rights owner must provide the information promptly.[166] The agreement does not require test transactions as part of the complaint submission.[167] Nor does the agreement require any pre-complaint direct communication between the rights owner and the accused merchant.

157. *See RogueBlock*, *supra* note 152.

158. *Payment Processor Initiative & Portal Program*, *supra* note 153 (stating that the annual fee for participation in the program is $6000, and that the setup and maintenance fee is $3900).

159. *Id.*

160. *See* EXECUTIVE SUMMARY, *supra* note 150, at 5 (reproducing a screen shot of the standardized form).

161. *Id.* at 4.

162. *See Payment Processor Initiative & Portal Program*, *supra* note 153.

163. *See* EXECUTIVE SUMMARY, *supra* note 150, at 7.

164. *See Payment Processor Initiative & Portal Program*, *supra* note 153.

165. Best Practices for Payment Processors, *supra* note 125, at 1–2.

166. *Id.* at 2.

167. *Id.* at 1.

Upon receiving a complaint, the payment processor must conduct an investigation.[168] If the payment processor is of a type that deals only indirectly with merchants through banks known as acquirers, which recruit merchants into card programs, then the relevant acquirer is responsible for conducting the investigation.[169] MasterCard and Visa are structured in this way.[170] For payment processors that interface directly with merchants (e.g., PayPal, Diners Club, and American Express), the payment processor is itself responsible for conducting the investigation.[171] Once a party files a complaint, the agreement puts the onus on the accused merchant to produce "credible evidence" that it is not engaged in infringing transactions.[172] If the merchant fails to respond or doesn't meet its burden, or if the party conducting the investigation "determines in its reasonable opinion that the merchant is engaged in sales of Illegitimate Products," then the merchant must block future infringing transactions.[173] If the merchant continues to engage in such transactions, then the payment processor or the acquiring bank "shall suspend or terminate payment services to that merchant with United States account holders."[174] The agreement contemplates additional "appropriate remedial measures" but does not specify them.[175] Termination is the typical sanction, as revealed in the IACC's FAQ for the Portal Program:

- What happens after a violation is reported?

  First, the IACC staff confirms that your Claim Report includes all the data necessary to proceed. Once that is done, a Trace Message[176] will be initiated to help

168. *Id.* at 2.

169. Systems structured in this way are known as four-party, or open, payment systems, because they operate through relationships with consumer-facing issuing banks (a.k.a. issuers) and merchant-facing acquiring banks (a.k.a. acquirers). *See id.* at 3. Issuing banks issue payment cards to consumers, and acquiring banks enroll merchants into card programs. *Id.* In a four-party system, the payment processor has no direct relationship with either merchants or cardholders. *Id.*

170. *See id.*

171. PayPal, Diners Club, and American Express are three-party, or closed, payment systems because they interface directly with merchants and consumers. *See id*. In a three-party system, the payment processor issues cards, recruits merchants, and processes transactions. *Id.*

172. *Id.* at 2.

173. *Id.*

174. *Id.*

175. *Id.* at 3.

176. For clarification,

> [a] 'trace message' is an attempt to make an online purchase using a valid, yet set-to-decline credit card. It is similar to a test purchase, but because the payment is declined, no goods are delivered. The purpose of a trace message is to assist the Card Network in identifying the merchant account associated with the

> identify the merchant processing for the rogue website. . . .
>
> - How do I know the results of my submitted claims?
>
> The information received back from the Trace Message will identify the merchant processing the transactions. *Typically, that merchant is then terminated*—though in some cases, the offending content can be removed. . . .[177]

In 2013, the IACC reported that 26,000 payment channels[178] identified on 7500 accused websites and more than 2100 individual merchant accounts had been terminated.[179]

For merchants who believe they have been wrongly sanctioned, the agreement requires payment processors to "have a process in place to allow for prompt review of remedial measures."[180] The agreement is silent, however, as to what or how much process is due when a merchant requests a review. No provision exists for third-party review or for a stay of termination pending resolution of the review.[181] In cases where the merchant disputes termination and the payment processor or acquiring bank reasonably concludes that the accused merchant is operating legitimately, the agreement implicitly contemplates that the payment processor may nevertheless impose or sustain termination if the rights owner is willing to indemnify it for any resulting legal liability.[182] As

---

[accused] website.

EXECUTIVE SUMMARY, *supra* note 150, at 6 n.5.

177. *Payment Processor Initiative & Portal Program*, *supra* note 153 (emphasis added).

178. A website has multiple payment channels if it accepts cards or payments from multiple payment processors. *See* Liz Gulsvig, *What's a Payment Channel?*, FORTE BLOG (May 5, 2014), https://www.forte.net/blog/whats-payment-channel/ ("A payment channel is basically any way that a customer might make a payment or anywhere that you (as a merchant) might accept a payment.").

179. *See Role of Voluntary Agreements*, *supra* note 137, at 56 (written testimony of Robert C. Barchiesi, President, IACC).

180. Best Practices for Payment Processors, *supra* note 125, at 3.

181. This is in contrast with the CAS, which provides for a stay of sanctions pending review. *See* Bridy, *Graduated Response*, *supra* note 22, at 53–54 (explaining the process for appealing a mitigation measure in the CAS).

182. *See* Best Practices for Payment Processors, *supra* note 125, at 3 ("A Payment System Operator may request a written agreement by the Right Holder to support the Payment System Operator fully in connection with a dispute where, in the Payment System Operator's reasonable opinion, the merchant provides credible evidence supportive of the merchant's position that it is not engaged in illegal conduct, including by defending, holding harmless and indemnifying the Payment System Operator for any costs, expenses (including legal fees) or liabilities arising in connection with such dispute.").

discussed more fully in Section II.B below, this risk-shifting provision effectively gives the complaining rights owner final say over termination decisions. As of October 2012, no complaints submitted through the Portal Program had been disputed.[183]

B. *The Protocol for Rights Owners*

The first best practice to which rights owners agree on their side of the bargain is that they will operate in good faith in identifying culpable websites.[184] The remaining best practices for rights owners are directed to streamlining the logistics of the notice-and-termination protocol described above.[185] Rights owners that are members of trade associations must channel their notices through those trade associations, which are designated as "channeling associations."[186] Channeling associations are expected to consolidate notices before presenting them to payment processors.[187] For cases in which a payment processor requires additional information, rights owners must designate a single point of contact and respond expeditiously to requests for additional information.[188] Participating channeling associations agree to develop and use a standardized form or system for submitting complaints and a standardized coding system to identify different types of infringement, such as "unauthorized copyright download, unauthorized copyright streaming, counterfeit goods, [and] circumvention devices."[189] For accused sites that accept payments from more than one payment processor, channeling associations are expected to provide concurrent notice, when possible, to all of the implicated payment processors, so that each is aware of the others' investigations.[190]

To all appearances, the IACC's Portal Program was purpose-built to operationalize the agreement, and the IACC single-handedly fulfills the protocol's channeling function for the large number of corporate trademark and copyright owners that are its members.[191] The IACC's member trademark owners include frequently knocked-off luxury brands such as Coach, Louis Vuitton Malletier, and Hermes.[192] The member copyright owners include the major recording labels and their trade

183. EXECUTIVE SUMMARY, *supra* note 150, at 12.

184. Best Practices for Rights-Holders, *supra* note 148, at 1.

185. *See id.* at 1–2.

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.* at 2.

191. For a complete list of the IACC's members, see *Member Brand Owners*, IACC, http://www.iacc.org/member_brands.html (last visited July 5, 2015).

192. *Id.*

association (the RIAA), the major movie studios and their trade association (the MPAA), and the major entertainment software distributors and their trade association (the ESA).[193] To view the extensive list of corporate rights owners that belong to the IACC is to appreciate the rationale for channeling in the best practices framework; without it, the protocol would be unmanageably inefficient.

III. SOME NORMATIVE CONSIDERATIONS

As voluntary enforcement agreements multiply at the urging of Congress and IPEC, advocates of balance and transparency in the intellectual property system have reason to be vigilant about their impacts on public access to physical and digital products online. The intermediaries that are parties to these agreements collectively exercise tremendous control over the Internet's universe of accessible content. If the agreements and their notice-and-sanction protocols were guaranteed to reach only "Illegitimate Products" and their purveyors, there would be no cause for concern. Because there is no such guarantee, however, and because the very point of these agreements is to facilitate the fast removal of large quantities of content, the protocols themselves should incorporate robust checks for preventing overreach and mistake. This Part considers the nature and adequacy of those checks to prevent extraterritorial application of expansive U.S. intellectual property laws and to insure that accused merchants do not have their payment services unfairly terminated.

A. *Extraterritoriality*

For rights owners, the appeal of payment blockades lies largely in their ability to reach, in SOPA's parlance, "foreign infringing sites."[194] Such sites are beyond the jurisdiction of U.S. authorities because their domain names are registered outside the United States and their operators and servers are physically located abroad.[195] If there is a conflict of

193. *Member Associations*, IACC, http://www.iacc.org/member-associations.html (last visited July 5, 2015).

194. *See* SOPA, H.R. 3261, 112th Cong. § 102(a) (1st Sess. 2011) (defining "foreign infringing site").

195. With the passage of the Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008, websites with U.S.-registered domain names became subject to in rem seizure and forfeiture by the U.S. government, even when their operators and servers are located abroad. *See* 18 U.S.C. § 2323 (2012) (providing for civil forfeiture of "property used . . . in any manner or part to commit or facilitate the commission of [any criminal copyright or trademark infringement]"); *see also* Bridy, *Carpe Omnia*, *supra* note 9, at 708–12 (discussing the PRO-IP Act and Operation In Our Sites, the U.S. Department of Homeland Security's domain name seizure program for domestically registered domain names); Jack Mellyn, *"Reach Out and Touch Someone": The Growing Use of Domain Name Seizure as a Vehicle for the Extraterritorial*

intellectual property laws between the United States and a jurisdiction in which a targeted site is registered and its operators and servers are located, the foreign operator of the targeted site and the site's non-U.S. customers could become indirectly subject to U.S. law through the imposition of a voluntary payment blockade.[196] Voluntary payment blockades can thus operate as a vehicle for the extraterritorial application of U.S. intellectual property laws, which can be significantly friendlier to rights owners than laws in other jurisdictions.[197] Under domestic judicial precedents, U.S. copyright law can have no extraterritorial effect.[198] Federal trademark law, on the other hand, can have extraterritorial effect, but only in very limited circumstances.[199] If payment processors are to avoid becoming copyright and trademark norm exporters for the benefit of U.S.-based rights owners, online payment blockades must be "zoned" to reach only transactions involving U.S. customers attempting to procure materials that are infringing or counterfeit under U.S. law.[200]

Problems of extraterritoriality were at the forefront in the case of AllofMP3.com, an online music store hosted in Russia and operated by Russian nationals.[201] The site sold millions of unauthorized downloads of copyrighted songs for a tiny fraction of the price charged by licensed

---

Enforcement of U.S. Law, 42 GEO. J. INT'L L. 1241, 1255 (2011) (arguing that U.S. domain name seizures violate established principles of domestic and international law, including norms governing jurisdiction to prescribe).

196. *Cf.* MacCarthy, *supra* note 19, at 1091–92 (pointing out that legal disputes involving cross-border online transactions can be complex for payment processors to assess and navigate when the merchant and the customer are in different jurisdictions and either the laws in the two jurisdictions are not the same or the legal situation in one country differs from that of the other).

197. *See, e.g.*, *id.* at 1095 (noting that in one case, "a local court ordered a local bank to continue to provide payment services" despite the fact that "these transactions would still be illegal in virtually every other country in the world").

198. Kirtsaeng v. John Wiley & Sons, Inc., 133 S. Ct. 1351, 1376 (2013) (stating that the Copyright Act does not apply extraterritorially); Perfect 10, Inc. v. Yandex N.V., 962 F. Supp. 2d 1146, 1153 (N.D. Cal. 2013) (holding that "foreign-hosted images are extraterritorial and not actionable under the [Copyright] Act").

199. *See, e.g.*, Wells Fargo & Co. v. Wells Fargo Express Co., 556 F.2d 406, 428 (9th Cir. 1977) (holding that federal trademark law may reach foreign activities if they have the requisite effect on U.S. commerce).

200. The principle that the Internet should be zoned to enable territorial sovereigns to enforce laws and adjudicate disputes goes back to the Internet's early days and to debates over restrictions on sexually explicit speech. *See* Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951, 1953 (2005) ("Technologies should be available to enable Internet participants to respect the rule of law in states where their Internet activities reach.").

201. *See* First Amended Complaint for Declaratory and Injunctive Relief and Damages at 6, Arista Records LLC v. MediaServices LLC, No. 06 Civ. 15319 (NRB), 2008 WL 563470 (S.D.N.Y. Feb. 25, 2008). The company registered the domain name for the website, however, in the United States. *Id.* at 4 (stating that the company registered the domain name with Register.com, Inc., a New York corporation).

distribution channels like iTunes.[202] In December 2006, U.S.-based record labels sued the site's operator, MediaServices LLC, in federal district court in New York for $1.65 trillion in damages for direct and secondary copyright infringement.[203] Under U.S. copyright law, the site was operating illegally.[204] Under Russian law, however, it was not.[205] Having no corporate presence in the United States, MediaServices elected not to answer the complaint.[206] Instead, it published a defiant statement on AllofMP3.com asserting the legality of its operation under Russian law and its right not to submit to the jurisdiction of New York courts.[207] It refused to accept service of process in Russia under Russian rules of procedure, and it opposed the plaintiffs' motion for authorization of substituted service in the United States under the Federal Rules of Civil Procedure.[208] After the judge in the case granted the labels' motion and authorized substituted service on MediaServices' New York attorneys, MediaServices moved to quash the substituted service.[209] It was bound

202. *See* Erik Larson, *Music Industry Drops Copyright Suit Against Russian Music Site*, BLOOMBERG (May 23, 2008, 5:45 PM), http://www.bloomberg.com/apps/news?pid=newsarchive&sid=as0feZVmo0_A ("The Web site had 5.5 million subscribers, who paid between 10 and 20 cents per song, compared with 99 cents charged by Apple Inc.'s online iTunes store.").

203. *See* Michael Arrington, *AllOfMP3 Responds to RIAA's $1.65 Trillion Lawsuit*, TECHCRUNCH (Dec. 27, 2006), http://techcrunch.com/2006/12/27/allofmp3-responds-to-riaas-165-trillion-lawsuit/ (reporting on the filing of the suit).

204. Bush administration officials reportedly called the site a "poster child for Internet music piracy." Larson, *supra* note 202.

205. *See Court Acquits AllOfMp3.com Site Owner*, CNN (Aug. 15, 2007, 10:46 AM), http://www.cnn.com/2007/TECH/biztech/08/15/russia.site.reut/index.html?eref=rss_tech (reporting on the Russian court's decision that the site's operator, Denis Kvasov, was not liable for copyright infringement because he paid a portion of the site's revenue to "ROMS, a Russian organization which collects and distributes royalties for copyright holders").

206. Arista Records LLC v. MediaServices LLC, No. 06 Civ. 15319 (NRB), 2008 WL 563470, at *1 (S.D.N.Y. Feb. 25, 2008) ("MediaServices has no known corporate presence in the United States.").

207. Arrington, *supra* note 203 ("This suit is unjustified as AllofMP3 does not operate in New York. Certainly the labels are free to file any suit they wish, despite knowing full well that AllofMP3 operates legally in Russia. In the meantime, AllofMP3 plans to continue to operate legally and comply with all Russian laws.").

208. *See MediaServices*, 2008 WL 563470, at *1–*2 (explaining the steps plaintiffs took to try to effect service of process in Russia and holding that there was no point in requiring plaintiffs to serve process pursuant to the Hague Service Convention because judicial cooperation between the United States and the Russian Federation had long since been suspended, and Russian authorities would have refused service).

209. *See* Notice of Motion to Quash Service or, in the Alternative, to Dismiss the Amended Complaint for Insufficiency of Service of Process at 1–2, *MediaServices*, No. 06-15319.

and determined not to litigate the case on its merits in the United States under U.S. law.[210]

Covering all their bases, and likely anticipating the tooth-and-nail fight over jurisdiction in New York, the record labels were already pursuing extrajudicial (i.e., private and political) remedies when they filed the suit. In September 2006, the International Federation for the Phonographic Industry (IFPI) successfully prevailed upon Visa and MasterCard to voluntarily stop processing payments for the site.[211] In addition, the U.S. Trade Representative pressured Russia to amend its law to illegalize the site as a soft condition for entry into the World Trade Organization.[212] Although Russia did later amend its law, the site-wide payment blockade went into effect before the change occurred.[213] In the interim, Visa and MasterCard were enforcing U.S. copyright law in Russia and blocking transactions that were legal in Russia.[214] MediaServices sued Visa in Russian court for breach of Visa's terms of service and won.[215] The victory was moot, however, in light of both the intervening change in Russian law and the pre-judgment impact of the

210. If the underlying events in the case had occurred after the launch of Operation in Our Sites in 2010, the AllofMP3.com domain name, by virtue of its registration in the United States, would have been eligible for in rem seizure at the labels' request by the Department of Homeland Security on the ground that it facilitated criminal copyright infringement. *See supra* note 195 and accompanying text.

211. Nate Anderson, *Music Industry Encouraged Visa to Pull the Plug on AllofMP3.com (Updated)*, ARS TECHNICA (Oct. 19, 2006, 11:59 AM), http://arstechnica.com/business/2006/10/8029/; *Credit Card Firms Cut off AllofMP3.com*, NBCNEWS.COM (Oct. 19, 2006, 7:44 AM), http://www.nbcnews.com/id/15323093/ns/technology_and_science-tech_and_gadgets/t/credit-card-firms-cut-allofmpcom/.

212. Thomas Crampton, *Russian Download Site Is Popular and Possibly Illegal*, N.Y. TIMES (June 1, 2006), http://www.nytimes.com/2006/06/01/world/europe/01cnd-mp3.html (reporting that "American trade negotiators darkly warned that the Web site could jeopardize Russia's long-sought entry into the World Trade Organization").

213. *See* Janko Roettgers, *AllOfMp3 Vows to Continue Despite Tougher Copyright Laws*, P2P BLOG (Sept. 1, 2006, 1:20 PM), http://www.p2p-blog.com/item-142.html.

214. *See* Jacqui Cheng, *AllOfMP3.com Down, but Not Out*, ARS TECHNICA (July 3, 2007, 11:51 AM), http://arstechnica.com/tech-policy/2007/07/allofmp3-com-breathes-its-final-breath/ (reporting that Russia agreed to modify its laws by June 1, 2007 to make the site illegal).

215. *See* Nate Anderson, *Russian Court Rules That Visa Must Process Payments for AllofMP3.com*, ARS TECHNICA (July 16, 2007, 1:59 PM), http://arstechnica.com/tech-policy/2007/07/russian-court-rules-that-visa-must-process-payments-for-allofmp3-com/ (reporting on the court's decision against Rosbank, the Russia-based acquiring bank that serviced AllofMP3.com's Visa account).

payment blockade.[216] During the pendency of the litigation, the site shut down, leading the labels to dismiss the suit in May 2008.[217]

Limiting the geographic scope of payment blockades can mitigate the problem of extraterritoriality and prevent U.S. law from becoming, de facto, the law governing every card-mediated transaction involving an accused online merchant, no matter where the merchant and its customers are located. Although mapping real-space territorial boundaries onto the Internet presents well-documented practical and theoretical challenges, legal frameworks for adjudicating conflicts of law in disputes involving cross-border transactions predate the Internet and have proven adaptable to online scenarios.[218] In the anti-piracy and anti-counterfeiting domains, MasterCard's payment blocking policy is representative of the approach payment processors have taken to handling conflicts of law between an online merchant's home jurisdiction and an online customer's home jurisdiction:

> If the Merchant is located in a country where the online sale of the alleged Illegitimate Product does not violate applicable country laws, the Acquirer must suspend or terminate acquiring sales by that Merchant to account holders of accounts issued in countries where the sale of the alleged Illegitimate Product is illegal or is otherwise prohibited by local law.[219]

Under this policy payments to a merchant from customers holding accounts in Country A are blocked if the transactions in question are illegal in Country A, even if the transactions are legal in Country B, the merchant's home country. If the transactions are legal in both Country A and Country B, then payments to the merchant in Country B from

---

216. Cheng, *supra* note 214.

217. *See* Larson, *supra* note 202 (reporting that the labels dismissed the suit because, in the words of a music industry spokesman, "[t]he site is now defunct and out of business, the result of a successful anti-piracy initiative").

218. The debate over extraterritoriality, choice of law, and spillover effects is seminal in the field of cyberspace law. *Compare* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996) (arguing for the exceptionalist view that the Internet's disregard for geographical boundaries "throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign"), *with* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 475 (1998) (arguing for the non-exceptionalist view that "from the perspective of jurisdiction and choice of law, territorial regulation of the Internet is no less feasible and no less legitimate than territorial regulation of non-Internet transactions").

219. *SOPA Hearing*, *supra* note 124, at 96–98 (Appendix A to statement of Linda Kirkpatrick) (explaining MasterCard's anti-piracy policies).

customers in Country A are processed.[220] Visa calls this principle "dual jurisdictional compliance": If the merchant and his customer are physically located in different countries, then the merchant must comply with the laws of the customer's country as if the merchant were physically located in that country.[221]

The best practices agreement provides for jurisdictionally selective blocking in the same manner as MasterCard's and Visa's policies; it requires payment processors, acting on an allegation of infringement under U.S. copyright or trademark law, to "suspend or terminate payment services to [the accused] merchant *with United States account holders*."[222] By limiting the blockade to payments from U.S. account holders, the best practices agreement does not prevent transactions that are legal for both the merchant and the customer in the countries where they are physically located.[223] This solves the extraterritoriality problem that confronted AllofMP3.com.

The agreement does, however, export U.S. law to the extent that a merchant located in a country where infringing-under-U.S.-law transactions are legal must treat those transactions as illegal when U.S. account holders are on the other side of them.[224] Such is the case, however, with cross-border transactions in physical space. For example, a seller of hashish in Amsterdam cannot legally ship product into Albany, even though a tourist from Albany is free to partake at an Amsterdam cafe. Considered in terms of negative impacts on the overall integrity of the global e-commerce system, the "zoned" payment blockades contemplated in the best practices agreement are preferable to the "zoned" DNS blocking protocols contemplated in COICA, SOPA, and PIPA, because payment blockades don't threaten to wreak havoc on the Internet's addressing system.[225]

---

220. PayPal has a similar conflict-of-laws policy governing online gambling transactions. *See PayPal Acceptable Use Policy*, PAYPAL, https://www.paypal.com/us/webapps/mpp/ua/acceptableuse-full (last updated Feb. 28, 2015) (prohibiting gambling transactions unless "the operator and customers are located exclusively in jurisdictions where such activities are permitted by law").

221. *See Online Pharmacy Guide for Acquirers*, VISA INC., at 10 (June 2014), http://usa.visa.com/download/merchants/Online-Pharmacy-Guide-for-Acquirers-June-2014.pdf ("If the . . . merchant is in a different country than the cardholder, the merchant must comply with the laws and regulations in the cardholder's country as if it were physically located in that country.").

222. Best Practices for Payment Processors, *supra* note 125, at 3 (emphasis added).

223. *Id.*

224. *Id.*

225. *See, e.g.*, Vixie, *supra* note 117; *see also* Steve Crocker et al., *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill*, DOMAININCITE.COM, at 3 (May 2011), http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf ("Mandated DNS filtering would be minimally effective and would present

B. *Fair Process*

What is most troubling about payment blockades is that they are imposed summarily by entities ill-suited to make on-the-fly determinations concerning the merits of intellectual property disputes, particularly with respect to websites where infringing and noninfringing content commingle. Payment processors can do a pretty good job of limiting blockades geographically through the principle of dual jurisdictional compliance; the less tractable challenge is to impose payment blockades justifiably—in a way that does not deny fair process to accused online merchants or impede the sale and distribution of lawful content and products to consumers who want them. Two features of the best practices protocol are concerning in this respect: (1) the protocol places the burden of proof on the accused merchant to prove her innocence following a complaint from a rights owner, and (2) the protocol substitutes the hurried judgment of a participating intermediary for the more deliberate judgment of a court. These two features make private enforcement much more efficient but also much less procedurally fair than civil judicial process.

The best practices agreement requires payment processors to investigate rights owners' complaints and puts the onus in an investigation on the accused merchant to prove to the satisfaction of the payment processor that the merchant is not engaged in infringing sales.[226] This arrangement reverses the ordinary allocation of burdens in a civil suit for infringement by requiring the accused party to prove its non-liability through the provision of "credible evidence."[227] The agreement leaves it to the discretion of a payment processor to determine the nature and scope of its investigations.[228] On that point, the agreement does not appear to contemplate much beyond the payment processor's asking the merchant to "provide written evidence that it has the right to legitimately sell the product in question."[229] Just as the agreement doesn't require a rights owner to perform test transactions before submitting a complaint, it doesn't require a payment processor to conduct test transactions in the

technical challenges that could frustrate important security initiatives. Additionally, it would promote development of techniques and software that circumvent use of the DNS. These actions would threaten the DNS's ability to provide universal naming, a primary source of the Internet's value as a single, unified, global communications network.").

226. Best Practices for Payment Processors, *supra* note 125, at 2–3.

227. *Cf.* Arrow Novelty Co. v. ENCO Nat'l Corp., 393 F. Supp. 157, 160 (S.D.N.Y. 1974), *aff'd*, 515 F.2d 504 (2d Cir. 1975) (describing the ordinary allocation of burdens in a civil suit for infringement).

228. *See* EXECUTIVE SUMMARY, *supra* note 150, at 6 (stating that each payment processor resolves investigations in accordance with its own internal policies and procedures).

229. *See* Best Practices for Payment Processors, *supra* note 125, at 2.

course of an investigation.[230] The payment processor performs both investigative and adjudicative functions, taking findings of fact and conclusions of law about copyright and trademark infringement out of the hands of juries and judges.

An accused merchant's avenue of redress also detours around the courthouse. If the merchant wants to contest the outcome of a payment processor's investigation or the imposition of a sanction, its appeal is to the payment processor, which owes it a "prompt review" under the terms of the agreement.[231] The agreement doesn't specify either temporally or substantively what review will suffice. If a rights owner wants to go to the mat in a particular case, however, the payment processor may do its bidding, in spite of a reasonable belief that the merchant is not engaged in infringement, if the rights owner agrees to defend, indemnify, and hold the payment processor harmless for the contested blockade.[232] If the rights owner is willing to assume the risk of suit, the agreement is such that the payment processor can impose a payment blockade and more or less wash its hands of any adverse legal consequences. That arrangement creates an incentive for payment processors to over-block merchants and leaves final decisions about disputed blockades in the hands of complaining rights owners. Whether, and to what extent, a revenue-related disincentive might offset that incentive to over-block is unclear. But given the fact that participating rights owners are themselves very high-value customers for payment processors, the business incentive to over-block may be irresistible.

To protect fairness in the face of efficiency, the best practices agreement for payment processors should incorporate a right of review by a legally competent neutral third party, as, for example, the CAS does.[233] The AllofMP3.com case demonstrated that a civil suit for breach of contract between a wrongfully blockaded merchant and his payment processor is always available as a backstop; however, if the goal of voluntary agreements as a genre is to provide for efficient, fair, and self-contained private resolution of online intellectual property disputes, then such agreements should always include the option for review by a neutral third party.

230. *See* EXECUTIVE SUMMARY, *supra* note 150, at 5.

231. Best Practices for Payment Processors, *supra* note 125, at 3.

232. *See id.*

233. *See* Bridy, *Graduated Response*, *supra* note 22, at 53–54 (explaining that a broadband user subject to a "mitigation measure" within the CAS has the right to appeal the sanction to a third-party arbitrator before the sanction is imposed).

IV. WORKING AROUND PAYMENT BLOCKADES: OTHER WAYS TO PAY

Any method of enforcing intellectual property rights online is only as effective as it is difficult to circumvent. For determined online infringers, getting around the obstacles that rights owners erect between them and free content has always been the name of the game.[234] Since before the dawn of the cat meme, technically savvy infringers have been leading rights owners on a merry chase across the Internet. In light of this rich history of evasion, answering the "circumvention question" is essential to assessing whether Internet payment blockades can actually make online infringement unprofitable.

If an online merchant is wholly or even predominantly reliant on traditional payment systems to realize revenue from transactions, then the imposition of a payment blockade will be fatal to that merchant's business. If, however, an online merchant can accept payments outside of traditional payment systems or can route card payments around payment blockades, then payment blockades become less effective, if not altogether neutralized, as an enforcement tool. This Part considers the use of vouchers and virtual currencies—specifically Bitcoin—to circumvent payment blockades.

A. *Vouchers for Downloads*

The use of vouchers to pay for downloads at AllofMP3.com followed shortly after payment processors instituted their blockade of the site.[235] A man alleged to be a U.K.-based agent of AllofMP3.com listed vouchers, valued at ten pounds apiece, for sale on both eBay and the dedicated URL allofmp3vouchers.co.uk.[236] The sale of vouchers on eBay was a means of co-opting a legitimate marketplace by tapping into its users' ability to make payments through the very payment processors that had cut off direct payments to AllofMP3.com. Each voucher contained an access code that enabled its user to download tracks from AllofMP3.com.[237] Before London police shut down the voucher scheme, it generated an estimated tens-of-thousands of pounds in revenue for the blockaded Russian site, all of it deposited into offshore accounts.[238] Although the voucher workaround was short-lived, it is a striking example of how

234. *Cf.* Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567 (2012) (discussing user strategies for circumventing geolocation tools to access regionally restricted content online).

235. *See* Cheng, *supra* note 214 (reporting that the payment blockade of AllOfMP3.com by major credit card companies "didn't stop voucher sites from popping up that allowed customers to purchase gift certificates to [the site]").

236. John Leyden, *Police Raid Ends AllofMP3.com Vouchers*, THE REGISTER (May 21, 2007, 1:00 PM), http://www.theregister.co.uk/2007/05/21/allofmp3_voucher_raid/.

237. *Id.*

238. *Id.*

nimble and creative determined infringers can be in the face of new enforcement strategies. The scheme's Russia-to-U.K. connection also highlights the global reach and organized nature of efforts to circumvent online anti-piracy and anti-counterfeiting enforcement.

B. *Bitcoin and Other P2P Virtual Currencies*

Compared to gimmicky voucher schemes, virtual currencies represent a more robust means of circumventing payment blockades. They have demonstrable legitimate uses and significant growth potential, though it remains unclear whether they will become mainstream.[239] Just as P2P electronic file-sharing protocols eliminate the need for a centralized intermediary to host files or maintain a searchable file index, P2P virtual currencies eliminate the need for third-party payment intermediaries to act as trusted authorities for processing and verifying transactions between merchants and customers.[240] They cut out the middleman. Bitcoin, the most well-known of the P2P virtual currencies, relies on public key encryption and a public ledger maintained by the system's participants to log each transaction, thereby preventing individual Bitcoins from being double-spent.[241] By virtue of its reliance on public key encryption, Bitcoin belongs to the subset of virtual currencies known as cryptocurrencies.[242]

Greatly simplified, a Bitcoin transaction works in the following way[243]: Say that Alice wants to transfer two Bitcoins to Bob. Alice and

239. *See* Timothy B. Lee, *This Senate Hearing Is a Bitcoin Lovefest*, WASH. POST (Nov. 18, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/18/this-senate-hearing-is-a-bitcoin-lovefest/ (reporting that witnesses at a hearing of the Senate Committee on Homeland Security and Governmental Affairs were attuned to potential criminal uses of Bitcoin but also mindful of the virtual currency's legal uses and innovative potential).

240. *See* P. CARL MULLAN, THE DIGITAL CURRENCY CHALLENGE: SHAPING ONLINE PAYMENT SYSTEMS THROUGH U.S. FINANCIAL REGULATIONS 86 (2014) ("Transactions on the Bitcoin network never need to circulate through a traditional financial institution or bank. The network operates peer-to-peer. A ubiquitous requirement of trust in government and central banks present in all government-issued fiat currency has been completely removed from Bitcoin transactions."); *see also* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN https://bitcoin.org/bitcoin.pdf, at 1 (describing, as the pseudonymous originator of the Bitcoin system, "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party").

241. *See* Morgen E. Peck, *Bitcoin: The Cryptoanarchists' Answer to Cash*, IEEE SPECTRUM, (May 30, 2012, 11:33 AM), http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0 (describing the verification and logging of transactions in the Bitcoin system to prevent double-spending).

242. Mariella Moon, *A Brief Attempt at Explaining the Madness of Cryptocurrency*, ENGADGET.COM (Jan. 21, 2015, 10:00 AM), http://www.engadget.com/2015/01/21/cryptocurrency-explainer/ (noting that Bitcoin was the first recognized cryptocurrency).

243. *See How Does Bitcoin Work?*, BITCOIN, https://bitcoin.org/en/how-it-works (last visited July 5, 2015).

Bob each use a Bitcoin client to join the Bitcoin P2P network. Alice and Bob each have a Bitcoin "wallet" on their computers. Inside each wallet, there is some number of virtual addresses, each of which has its own balance of Bitcoins. Alice publicly declares, via her client, that an address in her wallet wants to re-assign two of the Bitcoins associated with it to an address in Bob's wallet. Anyone on the network can verify the transaction between the address in Alice's wallet and the address in Bob's wallet using public-key cryptography. Using public-key cryptography, the network's participants verify the validity of Alice and Bob's transaction as a matter of consensus and append it to the public history of previously agreed-upon transactions. This public history, or ledger, is known as the block chain.[244] In the Bitcoin system, the block chain substitutes for a trusted third party as the means of verifying transactions.[245] Participants in the network who maintain the block chain are called miners and receive newly mined Bitcoins as compensation for their computational work.[246] Because this method of compensating those who do the work of keeping the currency secure and verified inheres in the system's architecture, the cost of trust is not passed on to those engaging in transactions.

Bitcoin is attractive to online merchants and their customers for a number of reasons. Because no third-party payment processors are involved in Bitcoin transactions, merchants pay no third-party transaction fees. They can retain their saved costs as profits or pass them along to customers in the form of lower prices. Merchants also have freedom from contract within the Bitcoin system. They do not have to agree, in exchange for the right to receive payments, to any standardized terms of service or codes of business conduct drafted by payment processors. Absent those contractual relationships, payment processors cannot unilaterally terminate merchants' ability to receive payments for any actual or alleged misconduct. By opting into the Bitcoin system and out of traditional payment systems, merchants can avoid becoming subject to the private law enforcement regime to which payment processors have agreed in the voluntary best practices agreement.

Cutting out the middleman as a private law enforcer cannot be equated, however, with wholesale evasion of law enforcement within the Bitcoin economy. Criminally inclined online merchants who have embraced the free-wheeling culture of Bitcoin in its immature phase will

244. Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System,* IEEE 1319 (2012), *available at* http://www.cs.kent.edu/~javed/class-P2P13F/papers-2013/P03-bitcoinanonymity-Reid.pdf.

245. *Id.* at 1319–20.

246. *See id.* at 1319 (describing how Bitcoin works)*; see also* Peck, *supra* note 241, at 3 (providing a detailed infographic of a Bitcoin transaction).

have a progressively harder time operating under the radar as Bitcoin's proponents intensify their efforts to make the system part of the financial mainstream.[247] When the FBI cracked down on the darknet online marketplace known as the Silk Road in late 2013, agents seized 144,000 Bitcoins with a market value of $28 million.[248] For more than two years before the FBI shut it down, the Silk Road was an online bazaar for all manner of contraband—from narcotics to guns to counterfeit goods and (presumably, child) pornography.[249] Bitcoin was the coin of the realm. The Silk Road's seizure by federal agents was a very public signal that the Bitcoin system will be brought by degrees within the financial regulatory and law enforcement framework outside of which it operated in its first few years of existence—and within which traditional payment networks have long operated. For legitimate merchants, participation in a more highly regulated and policed Bitcoin system will remain a way to avoid both transaction costs and compliance costs associated with traditional payment networks. Merchants who accept Bitcoin will increasingly have to do business within the limits of public law, but they will always remain free of the private-law obligations that go hand-in-glove with reliance on trusted payment processors.

Bitcoin appeals to buyers in online marketplaces primarily because Bitcoin transactions can afford a degree of privacy not associated with card payments. Traditional payment networks operate on the "know your customer" principle, which is a rule of verification required in part to safeguard the security of transactions and in part to ensure compliance with anti-money-laundering and anti-terrorism laws.[250] Payments in a traditional payment system are linked to verified personal accounts belonging to verified individuals. Bitcoin is not (and was not designed to be) intrinsically private or anonymous, despite public perception to the

247. *See generally* Stephen T. Middlebrook & Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813, 815 (2014) (reviewing recent regulatory developments with respect to virtual currencies generally and concluding, based on those developments, that "it is unrealistic to imagine that cryptocurrencies will not face regulation in the United States"); *see also* François R. Velde, *Bitcoin: A Primer*, CHI. FED LETTER, Dec. 2013, at 4 ("Should [B]itcoin become widely accepted, it is unlikely [to] remain free of government intervention, if only because the governance of the [B]itcoin code and network is opaque and vulnerable.").

248. *See* Samuel Rubenfeld, *US Says It Makes 'Largest-Ever' Bitcoin Seizure*, WALL ST. J. (Oct. 28, 2013, 2:47 PM), http://blogs.wsj.com/riskandcompliance/2013/10/28/us-says-it-makes-largest-ever-bitcoin-seizure/.

249. *See* Nicolas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*, 22 INT'L WORLD WIDE WEB CONF. 213 (2013), *available at* http://www2013.org/proceedings/p213.pdf.

250. *See* Möser et al., *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem*, 2013 APWG ECRIME RESEARCHERS SUMMIT 1, *available at* https://maltemoeser.de/paper/money-laundering.pdf (explaining the regulatory function of the "Know-Your-Customer" principle).

contrary.[251] The block chain, after all, contains a public record of every consummated Bitcoin transaction.

If Bitcoin users are careful, however, they can achieve a degree of privacy with Bitcoin that is unrealizable in a traditional payment system.[252] As one commentator explains, "Bitcoin is often described as providing pseudoanonymity, by creating enough obfuscation to provide users with plausible deniability."[253] The cause of obfuscation can be furthered if a user maintains multiple public keys and avoids revealing identifying information connected to her public keys.[254] It also helps for the payee to generate a new cryptographic key pair for each transaction.[255] For an added layer of obfuscation, third-party Bitcoin "mixers" or "laundries" offer Bitcoin users the ability to mingle their funds with a large pool of existing funds to make the origin of a particular transaction difficult to trace.[256] But even when users take steps to protect their privacy, researchers studying the extent of plausible deniability within the Bitcoin system caution that the system was not designed to protect anonymity and that able researchers can identify repeat users using purely passive analysis.[257] The upshot for online buyers seeking transactional privacy is that Bitcoin is potentially more anonymous than credit cards but less anonymous than cash.[258]

For as much as merchants and buyers see benefits in routing online transactions around traditional payment systems, the long-term sustainability of the Bitcoin system is uncertain.[259] Large fluctuations in

251. *See* Reid & Harrigan, *supra* note 244, at 1318 (commenting on the public misperception that Bitcoin is anonymous).

252. *See id.* at 1321 (explaining steps a Bitcoin user can take to protect his anonymity).

253. Peck, *supra* note 241.

254. Reid & Harrigan, *supra* note 244, at 1319.

255. *Id.*

256. *See* Möser et al., *supra* note 250, at 5–6 (evaluating the efficacy of three Bitcoin mixing services for anonymizing transactions); Jon Matonis, *The Politics of Bitcoin Mixing Services*, FORBES (June 5, 2013, 11:39 AM), http://www.forbes.com/sites/jonmatonis/2013/06/05/the-politics-of-bitcoin-mixing-services/ (describing different models for Bitcoin mixing).

257. *See* Reid & Harrigan, *supra* note 244, at 1325 ("Technical members of the Bitcoin community have cautioned that strong anonymity is not a prominent design goal of the Bitcoin system. However, casual users need to be aware of this, especially when sending Bitcoins to users and organizations they would prefer not to be publicly associated with.").

258. Ian Miers and his co-authors have described a fully anonymized cryptographic extension to Bitcoin called "Zerocoin." *See* Ian Miers et al., *Zerocoin: Anonymous Distributed E-Cash from Bitcoin*, *in* 2013 IEEE Symposium on Security and Privacy 397, *available at* http://www.ieee-security.org/TC/SP2013/papers/4977a397.pdf. They acknowledge, however, that "[their] work leaves several open problems." *Id.* at 408.

259. *See* Velde, *supra* note 247, at 3 (pointing out that as a fiduciary currency, "Bitcoin is free of the power of the state, but it is also outside the protection of the state," making it fragile).

value have beset the currency,[260] and the largest Bitcoin exchange, Mt. Gox, suspended trading and filed for bankruptcy in 2014.[261] At the time of its collapse, Mt. Gox announced that it could not account for 850,000 of its customers' Bitcoins, valued at $460 million.[262] It subsequently "found" 200,000 of them, but the rest remained unaccounted for as the company entered liquidation.[263] As the dust settles on the Mt. Gox fiasco, Bitcoin's backers are working to stabilize the currency's value, build consumer confidence in it, and bring it into regulatory compliance.[264] If they succeed, Bitcoin will continue to offer online merchants and buyers a viable alternative to traditional payment systems and a way around those systems' private anti-counterfeiting and anti-piracy operations.

CONCLUSION

Internet payment blockades are the fruits of a long-term, evolving strategy by corporate copyright and trademark owners to leave no intermediary behind when it comes to online intellectual property enforcement. Where judicial and legislative efforts failed to yield any binding public law requiring payment processors like MasterCard and Visa to act as intellectual property enforcers, "non-regulatory" intervention from the executive branch secured their cooperation as a matter of private ordering. The resulting voluntary best practices agreement prescribes a notice-and-termination protocol that extends the reach of U.S. intellectual property law into cyberspace, to merchants operating websites from servers and physical facilities located abroad. It also removes adjudications of infringement claims from the courts to the private sector, which raises issues of fairness and institutional competence. Like other forms of regulation by online intermediaries, payment blockades can be circumvented with the aid of disintermediating technologies. True to the Internet's founding purpose of redirecting data

260. *See* Kurt Avard, *Are Bitcoin Pricing Fluctuations Growing Pains or the Beginning of the End?*, THE MOTLEY FOOL (Feb. 12, 2014), http://www.fool.com/investing/general/2014/02/12/are-bitcoin-pricing-fluctuations-growing-pains-or.aspx (reporting on Bitcoin price fluctuations and their probable underlying causes).

261. Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014, 6:30 AM), http://www.wired.com/2014/03/bitcoin-exchange/ (reporting on the demise of Mt. Gox and attributing its failure to "a messy combination of poor management, neglect, and raw inexperience").

262. *Id.*

263. James Lyne, *$116 Million Bitcoins 'Found' at MtGox and How to Protect Your Wallet*, FORBES (Mar. 21, 2014, 10:34 AM), http://www.forbes.com/sites/jameslyne/2014/03/21/116-million-bitcoins-found-at-mtgox-and-how-to-protect-your-wallet/.

264. *See, e.g.*, Stan Higgins, *3 Forces Shaping Next-Generation Bitcoin Exchanges*, COINDESK (Aug. 31, 2014, 2:15 PM), http://www.coindesk.com/3-forces-shaping-next-generation-bitcoin-exchanges/; Wayne Lam, *Bitcoin Backers Work to Make It Mainstream,* FORBES (May 27, 2014, 10:36 AM), http://www.forbes.com/sites/techonomy/2014/05/27/bitcoin-backers-work-to-make-it-mainstream/.

flows around blocked or damaged channels, P2P virtual currencies like Bitcoin are empowering online merchants and their customers, at least for the time being, to run payment blockades.