PRIVATE ORDERING UNDER THREAT OF REGULATION

Jake Linford[*]

INTRODUCTION

In 2011, intellectual property (IP) owners lobbied for new laws that would have required internet firms to more proactively prevent infringement by foreign actors. These changes, embodied in a pair of federal bills, the Stop Online Piracy Act (SOPA) and PROTECT IP Act (PIPA),[1] would have required U.S.-based payment processors to take reasonable or technically feasible measures to prevent transactions between U.S. customers and the targeted domain name, whether or not that domain name was hosted in the U.S. or abroad.[2]

Given Congress' general receptivity to pro-IP lobbying,[3] IP owners might reasonably have expected the passage of SOPA and PIPA, even though advocates argued that the proposed scheme threatened to "break the internet."[4] It has long been conventional wisdom that copyright owners can turn to Congress for nearly automatic passage of laws that provide broad rights against infringers,[5] backed with high damages.[6]

---

* Assistant Professor of Law, Florida State University. My thanks to Derek Bambauer, Shawn Bayern, and David Levine for helpful feedback on this response.

1. Protect Intellectual Property Act (PIPA), S. 968, 112th Cong. (2011); Stop Online Piracy Act (SOPA), H.R. 3261, 112th Cong. (2011); Jake Linford, *The Institutional Progress Clause*, 16 VAND. J. ENT. & TECH. L., 533, 580–82 (2014) [hereinafter Linford, *Progress Clause*].

2. *See, e.g.*, Annemarie Bridy, *Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Perspective on ACTA, SOPA, and PIPA*, 30 CARDOZO ARTS & ENT. L.J. 153, 154 (2012) [hereinafter Bridy, *Policymaking*].

3. For example, Congress recently passed, and President Barack Obama signed into law, the Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified as amended at 18 U.S.C. § 1836 (2012)). The DTSA was enacted as an ostensible tool to fight cyberespionage, even though academics warned that it was unlikely to meet that goal and highly likely to have other negative consequences. *See* Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326) (Nov. 17, 2015); *see also* David S. Levine, *School Boy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation*, 72 WASH. & LEE L. REV. ONLINE 323, 326 (2015) (arguing the DTSA is underinclusive because it fails to directly address cyberespionage, and overinclusive because it would change trade secret doctrine to sanction the acquisition of trade secrets through what were formerly legal means).

4. Mark Lemley, David S. Levine & David G. Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34, 38 (2011). SOPA, for example, would have required domain name system authorities to prevent U.S. subscribers from viewing infringing sites by preventing domain names from resolving to the assigned Internet Protocol (IP) address. *See* H.R. 3261 § 102(c)(2)(A)(i).

5. *See* Jessica D. Litman, *Copyright, Compromise, and Legislative History*, 72 CORNELL L. REV. 857, 885 (1987); *see also* JESSICA D. LITMAN, DIGITAL COPYRIGHT 14 (2001) (describing how Congress, between 1990 and 1999, "added more than one hundred pages to the copyright statute, almost all of them billed as loophole-closers.").

6. Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. 439, 441 (2009).

However, in early 2012, support for SOPA and PIPA dissipated after millions of citizens, encouraged by Google, Wikipedia, and other internet heavyweights, petitioned their elected officials to oppose the bills.[7] After the demise of SOPA and PIPA, one might have reasonably concluded that direct intervention by Congress against internet vendors and intermediaries could be on its way out.

In *Internet Payment Blockades*,[8] Professor Annemarie Bridy explains that the battle instead shifted to a new front. Instead of Congress passing laws to regulate payment intermediaries directly, Professor Bridy describes how administrators in charge of IP policy have successfully pressured payment intermediaries to "voluntarily" shut off payments to websites that are loci of copyright or other intellectual property infringement.[9] As Professor Bridy recounts, the White House Office of the Intellectual Property Enforcement Coordinator (IPEC) persuaded payment processors (including American Express, Discover, MasterCard, PayPal, and Visa)[10] to enter an ostensibly voluntary best practices agreement with corporate intellectual property owners.[11] In accordance with the best practices agreement, IP owners provide notice of infringing sales by online merchants, as well as evidence that the IP owner owns the copyright or trademark in question and has notified the website operator of the infringement.[12] Payment processors agree to demand that vendors stop selling infringing goods,[13] and terminate relationships with vendors that "persist in intentionally selling Illegitimate Products."[14]

These agreements are ostensibly private agreements between payment processors and IP Owners.[15] As a result, government intervention isn't direct. Unfortunately, that also means many details about these agreements are not publicly available, and not subject to mandated disclosure through mechanisms like Freedom of Information

---

7. *See* Bridy, *Policymaking*, *supra* note 2, at 159.

8. Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523 (2015) [hereinafter Bridy, *Blockades*].

9. Bridy, *Blockades*, *supra* note 8, at 1524–25.

10. U.S. INTELLECTUAL PROP. ENF'T COORDINATOR, ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT 1 (2012) [hereinafter 2011 IPEC REP.], 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).

11. *See* Bridy, *Blockades*, *supra* note 8, at 1527.

12. *See* Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet at para. 3(c-d) (May 16, 2011) [hereinafter Best Practices Agreement].

13. *See id.* para. 7; *see also* Bridy, *Blockades*, *supra* note 8, at 1551.

14. Best Practices Agreement, *supra* note 12, at para. 8; *see also* Bridy, *Blockades*, *supra* note 8, at 1551.

15. Best Practices Agreement, *supra* note 12, at para. 4.

Act requests.[16]

Professor Bridy argues that adoption of the best practices agreement was effectively coerced by an unscrupulous threat to regulate if payment processors didn't sign on.[17] IPEC has a platform for suggesting new copyright and trademark laws to Congress each year.[18] Displeasing IPEC might therefore lead to a legislative response. Even worse, when the decision to terminate a vendor occurs outside of litigation, governed by terms that are not publicly accessible, accused infringers may not receive fair process. Vendors who are deemed infringers may find themselves unable to do business. Finding a new payment processor may be difficult, especially if most processors have signed on to the best practices agreement. But Professor Bridy finds hope that transactions using Bitcoin and other decentralized currencies might allow threatened online vendors to circumvent the payment blockades raised when payment processors sign on to the best practices agreement.[19]

Professor Bridy's analysis is mostly persuasive. In particular, her advice to beware administrators threatening regulation is well-taken. But there is some room for optimism, even when facing cajoled payment processors. Private ordering can be more efficient than government regulation,[20] even when it is encouraged externally rather than intrinsically inspired. For example, the negotiated agreement requires IP owners to take some reasonable steps in establishing IP rights, and requires fact finding by the payment processor or its intermediary, before sanctioning an allegedly infringing vendor.[21]

In addition, there are reasons to doubt that Bitcoin or similar cryptocurrencies will break payment blockades. Widespread adoption of Bitcoin or other cryptocurrencies may not happen. Bitcoin suffers from high complexity compared to standard currencies. It is also perceived as a technology optimized or primarily used for illicit transactions. In addition, the technology may process transactions without

16. *See* Bridy, *Blockades*, *supra* note 8, at 1547; *see also* David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 159–60 (2007) (describing how the Freedom of Information Act empowers citizens to request government-held information).

17. *See* Bridy, *Blockades*, *supra* note 8, at 1528.

18. 15 U.S.C. § 8111(b)(1)(F) (2012).

19. *See* Bridy, *Blockades*, *supra* note 8, at 1562.

20. *See* John McMillan & Christopher Woodruff, *Private Order Under Dysfunctional Public Order*, 98 MICH. L. REV. 2421, 2454 (2000) ("Private order therefore promotes economic efficiency by giving businesspeople the confidence to transact."); Charles J. Walsh & Alissa Pyrich, *Rationalizing the Regulation of Prescription Drugs and Medical Devices: Perspectives on Private Certification and Tort Reform*, 48 RUTGERS L. REV. 883, 889 (1996) (suggesting a plan to delegate some of the FDA's regulatory authority to private bodies in order to increase efficiency). *See generally* Irina D. Manta, *Privatizing Trademarks*, 51 ARIZ. L. REV. 381 (2009) (proposing privatized trademark registration as a means of improving efficiency).

21. Best Practices Agreement, *supra* note 12, at paras. 4, 6.

intermediaries, but it has not yet mastered a way to prevent fraud.

I. JAWBONING AND PRIVATE ORDERING

Professor Bridy's article lays bare "the ease with which the government can convince powerful corporate actors to do its bidding when behind-the scenes pressure is brought to bear."[22] The process is known by different names: proxy censorship,[23] soft censorship,[24] "new-school" speech regulation,[25] or "jawboning," where state actors seek to coerce a company "based on threatened action at the edges of or wholly outside their legal authority."[26] Jawboning is problematic because the outcome of threatened legal action may be uncertain, and the costs of the uncertainty are born by the target of the jawboning.[27]

A. *Payment Processors Lack Incentives to Protect Customers*

Jawboning may be particularly problematic when applied to internet intermediaries that provide access to expressive content. An intermediary may lack the incentive to protect third party content, and may concede to demands in cases where society might benefit if it did not yield.[28] Thus, when a state actor brings pressure, the cajoled party may act in its own self-interest with little concern for the needs of those whose speech or privacy could be restricted as a result of its decision.

Professor Bridy finds IPEC's jawboning of payment processors unprincipled in part because the threatened action may overreach the current contours of secondary liability in copyright and trademark law. As Professor Bridy explains, in 2007, the Court of Appeals for the Ninth Circuit undertook an exhaustive examination of secondary liability in *Perfect 10, Inc. v. Visa International Service, Association*.[29] In that case, the majority held, over a vigorous dissent by Judge Alex Kozinski, that Visa was neither contributorily nor vicariously liable for the infringement carried out by websites that used Visa to process payments.[30] After the Supreme Court denied Perfect 10's petition for

---

22. Bridy, *Blockades*, *supra* note 8, at 1526.

23. *See* 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).

24. *See* Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 870 (2012).

25. *See* Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2298 (2014).

26. Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51, 55 (2015) [hereinafter Bambauer, *Against Jawboning*].

27. *See id.* at 56.

28. *See id.* at 60.

29. *See* Bridy, *Blockades*, *supra* note 8, at 1535; Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788 (9th Cir. 2007).

30. *See* Bridy, *Blockades*, *supra* note 8, at 1529–30, 38.

certiorari,[31] IP owners shifted away from litigation and pursued legislative relief.[32]

Considering the case law, one might construe communication from IPEC to "threaten[] action at the edges of . . . [its] legal authority."[33] But we can better understand the strengths and limits of Professor Bridy's critique of IPEC's influence on payment processors by comparing that process to another recent example of soft coercion. In *Backpage.com, LLC v. Dart*,[34] the Seventh Circuit held that Thomas Dart, the Sheriff of Cook County, Illinois, exercised unconstitutional prior restraint on the speech of Backpage.com (Backpage) and its customers when he sent letters to Visa and MasterCard asking the companies not to process payments for the website, in light of what Dart insinuated was the companies' potential legal liability for ads for illegal services.[35]

Backpage is an online forum for classified ads. Backpage hosts ads for adult services, and Sheriff Dart suspected some of those ads offered illegal sex-related products or services like prostitution.[36] After receiving threatening letters from the sheriff, both Visa and MasterCard cut ties with Backpage.[37] The website sued Sheriff Dart for imposing informal prior restraint in violation of the First Amendment.[38] The court noted that the sheriff's goal was apparently to shut down Backpage "by suffocation, depriving the company of ad revenues by scaring off its payments-service providers," without concern for whether the pressure prevented legitimate as well as illegal offerings.[39] Sending the letters as

---

31. Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 553 U.S. 1079 (2008) (denying petition for certiorari).

32. *See* Bridy, *Blockades*, *supra* note 8, at 1540.

33. Bambauer, *Against Jawboning*, *supra* note 26, at 55.

34. 807 F.3d 229 (7th Cir. 2015).

35. Dart cited to the federal money laundering statute, 18 U.S.C. § 1956, as a basis for possible payment processor liability. *See* 807 F.3d at 232. Backpage may actually be insulated from some liability for sex trafficking even if it allows advertisers to solicit customers using its website under the Communications Decency Act of 1996, 47 U.S.C. § 230(c)(1). *See* Dart v. Craigslist, Inc., 655 F. Supp. 2d 961, 965–69 (N.D. Ill. 2009) (rejecting Dart's attempt to sanction Craigslist for similar advertisements because under the CDA, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"). *But see* 47 U.S.C. § 230(e)(1) ("Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of Title 18, or any other Federal criminal statute."). If Backpage is insulated from liability, the same would hold true for Visa and MasterCard. There can be no secondary liability without direct liability.

36. 807 F.3d at 230.

37. *See id.*

38. *See id.*

39. *Id.* at 231. Professor Bridy raises a similar example: Shortly after the Pentagon objected to the publication of leaked military and diplomatic documents by Julian Assange and Wikileaks, multiple payment processors including PayPal, Visa, and MasterCard stopped processing donations for Wikileaks. *See* Bridy, *Blockades*, *supra* note 8, at 1524–25. As Bridy

sheriff (rather than as a concerned, private citizen) was therefore an informal prior restraint, the use of coercive state power in a manner prohibited by the First Amendment.[40]

The Backpage case is somewhat analogous to the jawboning that drove the payment processors to the best practices agreement. In both situations, a state actor invites or coerces cooperation through threatened legal action. The sheriff's demand letters warned of potential dire consequences if payment processors continue to allow "suspected illegal transactions to . . . take place."[41] IPEC's conversations with payment processors in the shadow of potential legislative action led the processors to accept the responsibility to terminate relationships with repeat infringers.

Both cases also raise First Amendment implications. The Supreme Court has held that informal sanctions designed to suppress speech are unconstitutional. In *Bantam Books, Inc. v. Sullivan*,[42] the Court held that a state commission violated the First Amendment by sending threatening letters to a distributor of books the commission found obscene, even though the attempted censorship was informal.[43] Like the books in *Bantam Books*, the advertisements at issue in *Backpage* are close to core protected speech—and becoming closer, as the boundaries between commercial speech and other types of speech erode under the continued pressure of judicial review.[44]

The *Backpage* case also differs from the decision of payment processors to adopt best practices for dealing with infringement in a few critical respects. First, the First Amendment implications are stronger in

---

recounts, "staffers for U.S. lawmakers directly pressured MasterCard and Visa" to block payments to Wikileaks. *Id.* at 1525. Assange claimed that Wikileaks suffered a 95% drop in revenue as a result of the blockade. *Id.*

40. 807 F.3d at 231 ("But [Dart] is using the power of his office to threaten legal sanctions against the credit-card companies for facilitating future speech, and by doing so he is violating the First Amendment unless there is no constitutionally protected speech in the ads on Backpage's website . . . .").

41. *Id.* at 232.

42. 372 U.S. 58 (1963).

43. *See id.* at 64–72.

44. *Compare* Sorrell v. IMS Health Inc., 564 U.S. 552, 563-66 (2011) (applying heightened scrutiny and striking down regulation that barred the sale of doctors' prescribing information to pharmaceutical detailers), *with* Posadas de Puerto Rico Assocs. v. Tourism Co. of P.R., 478 U.S. 328, 340 (1986) (citing Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 561 (1980)) (holding "commercial speech receives a limited form of First Amendment protection"); *see also* Bates v. State Bar of Ariz., 433 U.S. 350, 364 (1977) (a "consumer's concern for the free flow of commercial speech often may be far keener than his concern for urgent political dialogue"); Linford, *Progress Clause*, *supra* note 1, at 542; Jane R. Bambauer & Derek E. Bambauer, *Information Libertarianism*, 105 CAL. L. REV. (forthcoming 2017) (recognizing the trend and arguing that it is beneficial because "when the state censors communication, the results are often counterproductive.").

the *Backpage* case than in the context of the best practices agreement. Current Supreme Court jurisprudence at the intersection of the First Amendment and copyright and trademark regimes suggests that courts are not likely to find First Amendment implications when the sales of counterfeit goods are blocked. The Court notes, for example, that "some restriction on expression is the inherent and intended effect of every grant of copyright."[45] The same can be said of trademark protection.[46] Nevertheless, the Court has held repeatedly that First Amendment concerns in copyright law can be sufficiently protected by regime-specific mechanisms, like the idea/expression doctrine or fair use.[47] The Court has therefore been unwilling to apply heightened First Amendment review of the federal copyright regimes.[48] But the Court has applied intermediate scrutiny to a provision that extended trademark-like rights in the term OLYMPIC to the United States Olympic Committee.[49]

Congress may lack the political capital to pass direct regulation that mirrors the obligations payment processors accepted under the best practices agreement. If such regulation were enacted, however, it would likely pass constitutional muster.[50] If jawboning is problematic when

45. Golan v. Holder, 132 S. Ct. 873, 876 (2012).

46. *See* Rogers v. Grimaldi, 875 F.2d 994, 998 (2d Cir. 1989) (holding "[t]hough First Amendment concerns do not insulate titles of artistic works from all Lanham Act claims, such concerns must nonetheless inform our consideration of the scope of the Act as applied to claims involving such titles"); Dr. Seuss Enters., L.P. v. Penguin Books USA, Inc., 924 F. Supp. 1559, 1571 (S.D. Cal. 1996), aff'd, 109 F.3d 1394 (9th Cir. 1997) (discussing potential First Amendment defenses to trademark liability).

47. *See* Eldred v. Ashcroft, 537 U.S. 186, 219 (2003) (the idea/expression dichotomy and the fair use defense are "traditional contours" of copyright protection); Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985) (First Amendment protections are "embodied in the Copyright Act's distinction between copyrightable expression and uncopyrightable facts and ideas," and in the "latitude for scholarship and comment" safeguarded by the fair use defense).

48. *See, e.g.*, 132 S. Ct. at 890–91 (rejecting Progress Clause and First Amendment challenges to a provision restoring protection to certain foreign-authored works); 537 U.S. at 219–20 (rejecting Progress Clause and First Amendment challenges to the Copyright Term Extension Act, which extended the copyright term for twenty years).

49. *See* San Francisco Arts & Athletics, Inc. v. USOC, 483 U.S. 522, 537 (1987) (holding that the Amateur Sports Act of 1978, which prohibited certain commercial and promotional uses of the term "Olympic," was not broader than necessary to protect a legitimate congressional interest and thus did not violate the First Amendment, even though the rights at issue were broader than standard trademark rights); *see also* Friedman v. Rogers, 440 U.S. 1, 16, 17 (1979) (holding that regulation to prevent the deceptive or misleading use of trade names did not violate the First Amendment). In the October 2016 term, the Court will decide whether the disparagement provision of the Lanham Act, 15 U.S.C. § 1052(a), which refuses registration to disparaging marks, is facially invalid. *See* Lee v. Tam, 137 S. Ct. 30 (2016) (granting writ of certiorari).

50. *But see* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1888–89

the state actor pressures behavior at the outer bounds, or even beyond legal boundaries,[51] then pressuring payment processors to discourage infringement and cut off repeat infringers may not be problematic. But a hypothetical regulation that would sanction payment processors for handling payments for any advertisements on Backpage.com regardless of the content of the advertisement would run afoul of the First Amendment.[52] Jawboning that leads payment processors to abandon Backpage full stop, irrespective of the legality of individual ads, is jawboning at its most invidious.

Second, in response to the pressure of Sheriff Dart, Visa and MasterCard stopped processing all payments for Backpage ads, whether or not those advertisements solicited custom for illegal behavior.[53] But under the best practices agreement, payment processors have the obligation to investigate (or direct an acquiring bank to investigate) whether a vendor is engaging in copyright infringement.[54] They accept the obligation to act only if the information gathered persuades them that the vendor is selling infringing goods and there is no "genuine issue" regarding the lawfulness of the merchant's sale.[55] As I will discuss below, the process isn't perfect, but there is a process in place that attempts to prevent chronic infringement without cutting off payments for plausibly legitimate sales.

Third, threatening litigation when the law has been interpreted in a way that makes the litigation specious is a particularly pernicious form of jawboning. But IPEC's jawboning took a much different form. Its ability to force action from payment processors depended on its success in pushing legislation through Congress[56]—a difficult task in a post-SOPA/PIPA world. Note the nature of the threat, if it can truly be considered a threat: IPEC effectively tells payment processors, "You do what I want you to do, or I'll tell Congress they ought to pass a law that makes you do what I want you to do." Conversely, Sheriff Dart raised the possibility that by processing payments for Backpage, payment processors will run afoul of current laws like a federal money-laundering statute.[57] A sitting sheriff armed with police power and an

(2000) (discussing First Amendment implications of the notice-and-takedown framework of the Digital Millennium Copyright Act, which requires internet service providers to takedown infringing content upon request from the IP owner).

51. *See* Bambauer, *Against Jawboning*, *supra* note 26, at 55–56.

52. *See* Backpage.com, LLC v. Dart, 807 F.3d 229, 230 (7th Cir. 2015).

53. *See id.* at 232, 236.

54. *See* Best Practices Agreement, *supra* note 12.

55. *See id.*

56. *See* Bridy, *Blockades*, *supra* note 8, at 1545 (arguing that because "IPEC makes specific legislative recommendations in its annual [Joint Strategic Plan], . . . the shadow of potential law hangs perennially over the private-sector conversations that it facilitates").

57. *See* 807 F.3d at 232.

aggressive interpretation of illegal behavior may well cause more direct and more immediate problems for payment processors than IPEC.

B. *Payment Processors Lack Incentives to Police Customers*

As discussed above, internet intermediaries and payment processors may not be motivated by self-interest to protect the speech or privacy interest of their customers. But the same is true of intellectual property rights. Internet and payment intermediaries are not directly incentivized to protect IP rights, especially in cases where failing to do so can be lucrative.

Recent cases like *Metro-Goldwyn-Mayer Studios Inc. v. Grokster*,[58] show how money can be made by turning a blind eye to infringement carried out by third parties,[59] or using that infringement as a mechanism to drive advertising traffic.[60] As others have noted, payment processors are a crucial link in the chain even if they are indirect contributors to infringement-driven business models.[61] And while secondary liability for payment processors may be in question,[62] U.S. law clearly sanctions the sales of counterfeit goods.[63]

C. *The Virtue of Private Ordering*

Professor Bridy is right to worry that jawboning puts undisclosed pressure on payment processors' private decisions.[64] Indeed, the exertion of pressure through jawboning strikes Professor Bridy as somewhat unprincipled, if not unscrupulous.[65] But there may be some hidden virtues in direct conversations between payment processors and IP owners, rather than directly imposed statutory solutions. Private ordering has its virtues. For instance, private ordering can be more

---

58. *See* 545 U.S. 913, 918–919 (2005).

59. *See, e.g.*, Jake Linford, *A Second Look at the Right of First Publication*, 58 J. COPYRIGHT SOC'Y U.S.A. 585, 642–43 (2011) [hereinafter Linford, *First Publication*] (discussing the risk of unauthorized copying and distribution a copyright owner faces when deciding whether to post her work online).

60. *See, e.g.*, Jake Linford, *Scarcity of Attention in a World Without Copyright* (2016) (draft on file with author).

61. *See, e.g.*, Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788, 811 (9th Cir. 2007) (Kozinski, J., dissenting); *cf.* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 222 (2006).

62. *See supra* notes 28–30 and accompanying text.

63. *See, e.g.*, 4 MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 25:10 (4th ed. 2016) ("If a product is a 'counterfeit,' consequences can include: criminal prosecution; ex parte civil seizure; more onerous importation penalties; and increased civil monetary recoveries, such as statutory damages.") (citations omitted).

64. *See* Bridy, *Blockades*, *supra* note 8, at 1545 ("In light of" the ability of IPEC to make legislative recommendations to Congress, "voluntary agreements [are] a form of regulation by arm-twisting.").

65. *See id.* at 1545–46.

efficient than regulation in some contexts, even if that private ordering occurs in the shadow of threatened regulation. Society and even vendors may benefit when payment processors actively negotiate the scope of best practices, and retain some discretion in how to implement the agreement. It is true that uncertainty about IP liability may sometimes cut against the merchant, especially considering the charge that IP owners have a tendency, and the incentive, to overclaim. Ensuing risk averse choices by payment processors may leave some vendors without a payment intermediary. But it is equally problematic to presume that a payment processor is obligated to deal with an entity whose behavior may run afoul of U.S. copyright or trademark law, whether or not the payment processor would be contributorily or vicariously liable for that behavior.[66]

If we assume that jawboning creates de facto regulation, direct conversations between payment processors and IP owners provide an opening for payment processors to shape the de facto regulation. One of the difficulties of the public choice account of the creation of IP laws generally is that not everyone can pay to play. Some stakeholders get left out of the discussion.[67] Jawboning which leads to private ordering affords each payment processor some discretion to decide how best to implement the responsibility to investigate alleged infringement by vendors, and what to do when they find it.

One could read Professor Bridy's article as a call to give preference to litigation or lobbying to handle all potential disputes. But those are not the only, or necessarily the fairest or most efficient means to resolve these conflicts. In fact, parties are encouraged to find negotiated resolutions to legal disputes where possible.[68] If payment processors find credible a threat by the government to regulate their industry, and chose to preempt the regulation with private ordering, negotiation may lead to better tailored responses. Each payment processor can choose to implement the best practices as they see fit, and if they do not coalesce

66. *See, e.g.*, Jason Mazzone, *Copyfraud*, 81 N.Y.U. L. REV. 1026, 1026 (2006).

67. *See* David S. Levine, *Transparency Soup: The ACTA Negotiating Process and "Black Box" Lawmaking*, 26 AM. U. INT'L L. REV. 811, 812 (2011) (documenting efforts to keep secret details about the recently negotiated Anti-Counterfeiting Trade Agreement); Jessica D. Litman, *Copyright Legislation and Technological Change*, 68 OR. L. REV. 275, 299 (1989) ("Throughout the various conferences, interests that were absent from the bargaining table were shortchanged in the compromises that emerged.").

68. *See* Kathleen C. Engel & Patricia A. McCoy, *A Tale of Three Markets: The Law and Economics of Predatory Lending*, 80 TEX. L. REV. 1255, 1353 (2002) ("Settlements offer the flexibility to forge creative solutions that are tailored to the loans and the borrowers in question."); *see also, e.g.*, Robbie v. City of Miami, 469 So. 2d 1384 (Fla. 1985) ("[S]ettlements are highly favored and will be enforced whenever possible.").

around the same terms,[69] the variance might well provide some vendors with payment options that have different levels of tolerance for alleged infringement.[70]

One might reasonably suspect that a threat to pass something like SOPA or PIPA that would directly reach payment processors is an empty threat after the dramatic failure of those Acts. But the processors themselves found the threat credible, or preferred to accept the "invitation" to self-regulate to the opportunity to oppose the legislation—a potentially costly process.[71] Such a deal is not per se unenforceable.[72] Indeed, contract law is full of examples where one party provides valuable consideration by forgoing an opportunity to sue another party. Whether the consideration is valid does not turn on whether the forbearing party could have successfully prosecuted its case, but instead whether the claim of right was subjectively reasonable and whether the party settling with the forbearing party believed it received some value from the transaction. For example, in *Military College Co. v. Brooks*,[73] a father agreed to settle a claim by a boarding school for tuition after the school dismissed his son for misconduct.[74] The court held that the promise not to sue for tuition was valuable consideration, even though there was some question as to whether the son was wrongfully dismissed, and thus whether the settled claim was valid.[75]

In addition, allowing providers of services some discretion in

---

69. *Contra* Henningsen v. Bloomfield Motors, Inc., 32 N.J. 358, 391 (1960) (finding unconscionable terms adopted by the "big three" U.S. automobile manufacturers that severely limited warranties, in part because consumers could find no seller providing better terms).

70. *Cf.* Linford, *First Publication*, *supra* note 59, at 654–55 (arguing that publishers and authors would benefit from the ability to consider the varied security profiles of competing online intermediaries when deciding how and whether to provide internet access to their copyrighted expression).

71. *See, e.g.*, Kreimer, *supra* note 23, at 27 (describing the danger of externalizing costs of resisting regulation of otherwise governable conduct on to intermediaries subject to direct regulation).

72. Note, however, that an agreement reached under duress is unenforceable. *See, e.g.*, Austin Instrument, Inc. v. Loral Corp., 272 N.E.2d 533, 537 (N.Y. 1971); Mark Seidenfeld & Murat C. Mungan, *Duress As Rent-Seeking*, 99 MINN. L. REV. 1423, 1426–27 (2015) (arguing that deals negotiated through "wrongful economic threats" should be unenforceable to the extent that the threats enable inefficient rent seeking).

73. 147 A. 488 (N.J. 1929).

74. *See id.* at 488–89.

75. *Id.* at 489 ("An agreement to pay money in compromise of a suit is valid, and that regardless of the validity of the plaintiff's demand."); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 74(1) (AM. LAW INST. 1981) (forbearance of a claim is valid consideration even if the claim or defense is doubtful, if that doubt is due to uncertainty as to facts or law, or the forbearing party believes the claim is valid). *But see* RESTATEMENT (FIRST) OF CONTRACTS § 76(b) (AM. LAW INST. 1932) (forbearance of an invalid is not valid consideration if the forbearing party lacks an honest and reasonable belief in its possible validity).

deciding with whom and how to deal is a well-established position in U.S. contract law. It would be problematic to suggest that a payment processor should be forced to continue processing payments for a vendor that persisted in engaging in illegal activity. Parties can and should be allowed to contract with one another in a manner that they see fit.

Professor Bridy also expresses concern that the best practices agreement threatens to make U.S. copyright and trademark law the default for all online transactions.[76] Professor Bridy highlights this possibility with a dispute that predates the best practices agreement. AllofMP3.com was a Russian website that sold mp3 downloads for a fraction of the price charged by authorized U.S. sellers.[77] AllofMP3.com was not compliant with U.S. law, but complied with Russian law.[78] An industry group nevertheless convinced payment processors to stop processing payments for the site.[79] The site shut down after Russian law changed, but the example highlights the potential extraterritorial reach of decisions by payment processors. If U.S. payment processors are handling international transactions, then "U.S. law [may] becom[e], de facto, the law governing every card-mediated transaction involving an accused online merchant, no matter where the merchant and its customers are located."[80]

Imagine, however, the counterfactual. If payment processors are not persuaded to stop payments to AllofMP3.com, then Russian copyright law becomes the default for online transactions, as U.S. consumers take advantage of much lower prices than authorized U.S. sellers can offer. Every default sets the terms under which subsequent transaction or regulation must occur,[81] and every default imposes some costs on subsequent transactions or regulations, unless transaction costs are

76. *See* Bridy, *Blockades*, *supra* note 8, at 1554–55 ("If there is a conflict of 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.").

77. *See id.* at 1555–56.

78. *See id.* at 1556 (citing *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")).

79. *See id*. at 1557.

80. *Id.* at 1558.

81. *See* Cass R. Sunstein, *Empirically Informed Regulation*, 78 U. CHI. L. REV. 1349, 1392 (2011) (citing Eric J. Johnson et al., *Framing, Probability Distortions, and Insurance Decisions*, 7 J. RISK & UNCERTAINTY 35, 48–50 (1993)).

zero.[82] Indeed, sometimes defaults are particularly sticky because many people will not choose to opt out of the default.[83] If U.S. law isn't the default, then Russian law becomes the default, with its norms of non-infringement and non-compensation for copyright owners.[84]

In reality, the voluntary action of payment processors provided a more finely-tuned outcome than either of the default positions described above. For example, as Professor Bridy reports, payment processors like MasterCard block transactions between foreign sellers and customers in the U.S. if the transaction violates U.S. law.[85] But payment processors do not block transactions between foreign sellers and foreign customers if the transaction is legal in their respective jurisdictions.[86] The voluntary regime effectively separates provision of services to U.S. consumers that would be infringing under U.S. law from sales to foreign consumers that would not be infringing under foreign law. As Professor Bridy acknowledges, this quasi-private ordering provides a better outcome than SOPA and PIPA, the legislation brought forward in Congress to deal with the perceived problem of extraterritorial infringement.[87]

Professor Bridy has also recognized the virtue of private ordering in the context of peer-to-peer infringement.[88] The Digital Millennium Copyright Act ("DMCA")[89] grants online service providers immunity from secondary liability for copyright infringement by their customers, if they take down on notice from copyright owners infringing content stored on the service provider's network at the direction of users.[90] But the takedown requirement doesn't reach infringement that is shared peer-to-peer, because the infringing material isn't stored anywhere that the service provider can reach it.[91] Content owners brought John Doe suits, sometimes against thousands of anonymous infringers, seeking to acquire the identities of consumers.[92] Some courts responded by

82. *See, e.g.*, Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 93 (1989).

83. *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 161–74 (2008).

84. *See* Bridy, *Blockades*, *supra* note 8, at 1556, 1559.

85. *See id.* at 1557.

86. *See id.* at 1558 (quoting *Stop Online Piracy Act: Hearing Before the Comm. on the Judiciary H.R. on H.R. 3261*, 112th Cong. 96–98 (2011) (Appendix A to statement of Linda Kirkpatrick, Group Head, Customer Performance Integrity, MasterCard Worldwide)).

87. *See* Bridy, *Blockades*, *supra* note 8, at 1559.

88. *See* Annemarie Bridy, *Is Online Copyright Enforcement Scalable?*, 13 VAND. J. ENT. & TECH. L. 695, 727 (2011) [hereinafter Bridy, *Scalability*].

89. Pub. L. No. 105-304, 112 Stat. 2877 (1998) (codified as amended at 17 U.S.C. § 512 (2012)).

90. *See* 17 U.S.C. § 512(c).

91. *See id.* § 512(a)(4).

92. *See* Bridy, *Scalability*, *supra* note 88, at 720–22.

severing defendants that had been improperly joined.[93] Pleas for Congress to amend the DMCA went unanswered, so service providers like Verizon made deals with content owners like Disney, offering to forward notices from Disney to Verizon customers.[94] Verizon was able to process Disney's complaints without violating customer privacy by disclosing customer identities.[95] As Professor Bridy notes, the direct negotiation between IP owners and service providers "serve[d] the interests of both privacy and efficiency."[96] Similar benefits can come from encouraging direct negotiation between IP owners and payment providers, even if an agency like IPEC helps open communication channels.[97] It is also possible that private ordering opens space for merchants to insert themselves into the negotiation. If a critical mass of merchants take issue with how one payment processor implements the best practices agreement, they can shift business to a different provider, or discuss potential changes collectively.[98]

Admittedly, one flaw of private ordering in crafting best practices for payment processors is that infringing vendors do not have a voice at the table. That would likely have been the case with regard to a legislative response as well.[99] The potential dissatisfaction of vendors with the best practices agreement might resemble the dissatisfaction of consumers subject to new terms of service pursuant to a change of terms clause. These terms are often adopted by credit card companies to provide the card provider with maximum flexibility, and enforced by courts over objections that they are unconscionable or otherwise

93. *See id.* at 723 (summarizing cases).

94. *See* Bridy, *Scalability*, *supra* note 88, at 726–27.

95. *See id.* at 726.

96. *Id.* at 727.

97. There are some who argue that IPEC is so firmly on the side of IP owners that its role in opening those channels is inherently problematic. *Compare* David Kravets, *U.S. Copyright Czar Cozied Up to Content Industry, E-Mails Show*, WIRED, Oct. 14, 2011, https://www.wired.com/2011/10/copyright-czar-cozies-up/ (reporting that IPEC head Victoria Espinel may have had a close relationship with content owners while IPEC brokered a private six-strikes deal between IP owners and online service providers), *and* Bambauer, *Against Jawboning*, *supra* note 26, at 77–78 (when IPEC was engaged with six-strikes negotiations, "Vice President Joe Biden convened a copyright enforcement meeting that included law enforcement, the IPEC, and content companies—but not ISPs"), *with* Mike Masnick, *President Obama Finally Gets Around to Nominating a New IP Czar*, TECHDIRT, Aug. 29, 2014, https://www.techdirt.com/articles/20140829/06225828360/president-obama-finally-gets-around-to-nominating-new-ip-czar.shtml (noting that while the former head of IPEC, Victoria Espinel, immediately took a lobbying job after leaving IPEC, she nevertheless "worked really hard to take opposing viewpoints into account").

98. *Cf.* Charles J. Goetz & Robert E. Scott, *Principles of Relational Contracts*, 67 VA. L. REV. 1089, 1132 (1981) (describing how franchisees collectively negotiated to limit unilateral termination in franchise contracts).

99. *See supra* note 66 and accompanying text.

problematic.[100]

The decision to extend or deny credit has a significant effect on consumers, but extending credit to the wrong consumers can have a negative effect on card issuers.[101] If credit card companies can decide whether to extend credit,[102] should the law prevent payment processors from deciding whether to process payments for repeat infringers? The assessment of risk—and the decision about whether to continue the relationship—properly belongs with the payment processor. If the processor can decide the procedure for ending a relationship with a vendor, fair process may be a non-issue, unless the payment processor breaches terms of its contract with a vendor.

Professor Bridy argues the systemic impact of allowing payment processors to exercise this discretion threatens the internet ecosystem.[103] In assessing whether this discretion conveys problematic "existential power [on] payment intermediaries,"[104] we must consider whether the best practices adopted by payment processors allow for unfair termination of vendors, or provide them with sufficiently fair process.

II. FAIR PROCESS UNDER THE BEST PRACTICES AGREEMENT?

Professor Bridy acknowledges that in a perfect world, private agreements like the best practices agreements would raise no cause for alarm.[105] But mistakes are likely inevitable. Lowering error costs often requires increasing enforcement costs.[106] Professor Bridy notes that because the best practices are designed to make it easy to quickly remove large amounts of infringing content, higher enforcement costs

---

100. *See generally* Jake Linford, *Unilateral Reordering in the Reel World*, 88 WASH. L. REV. 1395, 1413–14 (2013) (describing cases considering the enforceability of change of terms clauses).

101. *See* Adam J. Levitin, *Rate-Jacking: Risk-Based & Opportunistic Pricing in Credit Cards*, 2011 UTAH L. REV. 339, 363 (2011) (discussing risk faced by credit card providers when extending a line of credit).

102. The authority to deny credit is not without limits. For example, if an institution denies credit based on information obtained from a consumer reporting agency, section 615 of the Fair Credit Reporting Act requires the institution to send notice of the denial. ¶ 10-035 *Duties of Report Users*, FIN. PRIV. L. GD. P 10-035 (CCH), 2015 WL 6372996 (2016).

103. *See* Bridy, *Blockades*, *supra* note 8, at 1525.

104. *Id.*

105. *See* Bridy, *Blockades*, *supra* note 8, at 1560–61.

106. *See, e.g.*, Tun-Jen Chiang, *The Rules and Standards of Patentable Subject Matter*, 2010 WIS. L. REV. 1353, 1400 (2010) (citing Richard A. Posner, *Employment Discrimination: Age Discrimination and Sexual Harassment*, 19 INT'L REV. L. & ECON. 421, 423 (1999) ("Rules have higher error costs but lower administrative costs; standards have lower error costs but higher administrative costs. The relative size of the two types of cost will determine the efficient choice between the alternative methods of regulation in particular settings.")); *see also* Robert G. Bone, *Enforcement Costs and Trademark Puzzles*, 90 VA. L. REV. 2099, 2124 (2004).

should be required to lower potential error costs.[107] Other regimes designed to deal with problems of internet infringement, like the notice and takedown regime of the DMCA, or the Copyright Alert System, a framework for internet service providers to warn—and eventually sanction—customers who regularly engage in infringement, include options for judicial review. [108]

It is unclear whether the best practices agreement for payment processors provides that same option. The best practice agreement states that payment processors "shall have a process in place to allow for prompt review of remedial measures imposed" if a vendor or acquiring bank "disputes the allegations of infringement."[109] My attempt to acquire more detailed information from payment processors about the contours of this "prompt review" was not successful.

While I was unable to secure information directly from any payment processor about how they handle intellectual property disputes, some payment processors have posted online a description of their process. For example, according to a recent online publication, "Visa is committed to preventing the use of its payment brand and system for illegal transactions."[110] Visa's process includes directing an allegedly infringing merchant to cease selling goods identified as infringing by an IP owner, or terminating the merchant's account, if it receives evidence of repeat infringement.[111]

To initiate Visa's process, an IP owner must provide evidence of prior enforcement efforts, demonstrating "the IP Owner's own good faith attempts to enforce its IP rights."[112] Visa specifically contemplates that a cease-and-desist letter might indicate such a good faith attempt.[113] Visa also requires proof that the complaining owner has valid rights, including but not limited to trademark or copyright registration

---

107. *See* Joseph Scott Miller, *Error Costs & IP Law*, 2014 U. ILL. L. REV. 175, 182 (2014) ("[F]alse positives (erroneous grants of an IP entitlement) are systematically costlier than false negatives (erroneous denials of an IP entitlement).").

108. *See* Annemarie Bridy, *Graduated Response American Style: "Six Strikes" Measured Against Five Norms*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 53–55 (2012) (describing opportunities for neutral adjudication under the Copyright Alert System).

109. Best Practices Agreement, *supra* note 12, at para. 10.

110. *Intellectual Property*, VISA USA, usa.visa.com/legal/intellectual-property-rights.html (last visited Jan. 7, 2017) [hereinafter Visa IP Policy] (click on "Report intellectual property abuse" tab).

111. *See id.* (click on "Illegal transactions prohibited" tab).

112. *Id.* (click on "Evidence of Prior Enforcement Efforts" tab).

113. *See id.* Unfortunately, while sending a demand letter certainly provides evidence of an attempt to enforce IP rights, it does not necessarily evidence the existence of enforceable rights. *See, e.g.*, Irina D. Manta, *Bearing Down on Trademark Bullies*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 853, 854 (2012) (describing how trademark "bullies" send cease and desist letters based on legal claims that are spurious or non-existent).

certificates.[114] In addition, Visa also requires evidence that the allegedly infringing goods can be purchased using a Visa card.[115] Visa further demands a signed attestation under penalty of perjury, but doesn't specify to what the IP owner must attest.[116]

Some of the requirements Visa imposes on IP owners are similar to the steps required of copyright owners requesting takedown from an online service provider pursuant to the DMCA.[117] The party requesting takedown must assert, under penalty of perjury, that it represents a legitimate IP owner.[118] The complaining party must identify the work or works that are infringing with enough specificity for the service provider to locate them.[119] And the complaining party must assert a good faith belief that the material to be taken down is not authorized by the copyright owner, its agents, or the law.[120] At least one court has held this good faith belief requires the complaining party to consider whether the use of the work was fair use before sending a takedown notice.[121] These thresholds are not inconsequential. Courts have held that failure to observe DMCA formalities invalidates a takedown request.[122]

If the IP owner crosses these DMCA-style thresholds, Visa instructs an "acquiring bank," the entity with a direct relationship to the accused vendor,[123] to investigate allegations of IP infringement.[124] If the acquiring bank concludes that the merchant is selling infringing goods identified by the IP owner, and the merchant does not cease selling those goods, the acquiring bank is expected to stop processing Visa

---

114. *See* Visa IP Policy, *supra* note 110 (click on "Evidence of IP Rights" tab)

115. *See id.* (click on "Acceptance of Visa cards at the Merchant website" tab).

116. *See id.* (click on "IP owner's attestation" tab).

117. That's not to say the DMCA's policies are ideal. In fact, they are frequently criticized. *See* Jennifer M. Urban et al., *Notice and Takedown in Everyday Practice*, UC Berkeley Pub. L. Res. Paper No. 2755628 (2016), http://ssrn.com/abstract=2755628 (noting that the DMCA works differently for different actors, and identifying flaws in its current operation); *see also* Annemarie Bridy, *Three Notice Failures in Copyright Law*, 96 B.U. L. REV. 777, 783-790 (2016) (arguing that the DMCA's red flag knowledge standard under 17 U.S.C. § 512(c)(1)(A) fails to provide sufficient notice to online intermediaries). But it would not be surprising to see similar policies required by direction legislative intervention.

118. *See* 17 U.S.C. § 512(c)(3)(A)(i, vi).

119. *See id.* at § 512(c)(3)(A)(ii, iii).

120. *See id.* at § 512(c)(3)(A)(v).

121. *See* Lenz v. Universal Music Corp., 815 F.3d 1145, 1153 (9th Cir. 2016) ("[B]ecause 17 U.S.C. § 107 created a type of non-infringing use, fair use is 'authorized by the law' and a copyright holder must consider the existence of fair use before sending a takedown notification under § 512(c).").

122. *See, e.g.*, Hendrickson v. eBay Inc., 165 F. Supp. 2d 1082, 1089–90 (C.D. Cal. 2001).

123. Visa contracts with merchants through acquiring banks. *See* Bridy, *Blockades*, *supra* note 8, at 1551.

124. Payment processors like American Express do not use acquiring banks as intermediaries and must conduct their own inquiries. *See id*.

payments for the merchant.[125] On the other hand, if the merchant or acquiring bank provides evidence of a "genuine issue" regarding the lawfulness of the merchant's sale of the identified goods, Visa opts out of the conversation, passes the collected evidence on to the IP owner, and encourages the IP owner to address its concerns directly to the merchant or the acquiring bank.[126]

Visa also reserves the right to require the IP owner to indemnify or otherwise hold Visa harmless for attorneys' fees, costs, and damage incurred in connection with the dispute. Visa's publicly available explanation of its practices reserves the sole discretion to decide whether the IP owner must "defend, indemnify, and hold Visa harmless" against claims by the acquiring bank or the merchant regarding action taken.[127] Visa also reserves sole discretion to determine whether an IP owner must pay attorneys' fees, costs, and damages incurred by Visa or the acquiring bank in connection with the dispute.[128] The indemnification clause superficially resembles a bond to secure injunctive relief. As in other federal cases, IP owners seeking injunctive relief must post a bond to secure that relief.[129] If regularly applied, the indemnification clause should forestall some overclaiming by IP owners.[130]

But Visa's right to seek indemnification isn't exactly like a bond. In litigation, a bond must be paid in an amount deemed sufficient by a district court before a preliminary injunction will issue.[131] That amount is set in part to compensate the enjoined party if the injunction was improperly granted.[132] Visa's process is an ex post redistribution of costs, rather than an ex ante determination about the potential harm of an erroneously granted injunction. In addition, in litigation, a judge determines whether the IP owner is entitled to injunctive relief, weighing the burdens on the IP owner, the alleged infringer, and the

125. *See* Visa IP Policy, *supra* note 110.

126. *See id.*

127. *Id.* (click on "What if the Merchant defends its business?").

128. *See id.*

129. *See* FED. R. CIV. P. 65(c); Georgia Television Co. v. TV News Clips of Atlanta, Inc., 718 F. Supp. 939, 950 (N.D. Ga. 1989) (noting in a copyright infringement dispute, that "Rule 65(c) requires the posting of security in the sum as the Court deems proper for the payment of costs and damages as may be incurred or suffered by any party who is found to have been wrongfully enjoined or restrained").

130. *Cf.* Nintendo of Am., Inc. v. Lewis Galoob Toys, Inc., 16 F.3d 1032, 1037 (9th Cir. 1994) (allowing the wrongfully enjoined party to recover the injunction bond discourages parties from "requesting injunctions based on tenuous legal grounds").

131. *See* Thomas Patterson, *Litigation: The Bond Requirement for Preliminary Injunctions*, INSIDE COUNSEL (Sept. 5, 2013), http://www.insidecounsel.com/2013/09/05/litigation-the-bond-requirement-for-preliminary-in.

132. qad. inc. v. ALN Assocs., Inc., 781 F. Supp. 561, 562 (N.D. Ill. 1992).

public at large.[133] A process like Visa's instead leaves Visa and its acquiring banks with the responsibility of determining whether a vendor will lose its ability to process payments. There are no articulated standards for how Visa should evaluate relative costs, merely a statement that in cases with "genuine issues," it will opt out of the discussion and leave the IP owner and vendor to discuss the infringement directly.[134] The process outlined is imperfect, to be sure, but the burdens of production on owners are not inconsequential. And the imperfections do not justify stripping payment processors of the ability to decide how and whether to transact with vendors, irrespective of whether those decisions are made in the shadow of threatened legislation.

III. BREAKING BLOCKADES INTO BITS

Professor Bridy hopes that shifting transactions to Bitcoin or other cryptocurrencies might provide online vendors like AllofMP3.com the ability to reach consumers sans intermediation, which would insulate them from the decisions of payment processors to implement arrangements like the best practices agreement.[135] Bitcoin and other cryptocurrencies reduce the costs of validating transactions and mediating disputes as users contribute computer processing power to validate transactions,[136] "creating a public record of the chain of custody of each Bitcoin."[137] Satoshi Nakamoto, the programmer credited with

133. *See, e.g.*, Voice of the Arab World, Inc. v. MDTV Med. News Now, Inc., 645 F.3d 26, 34 (1st Cir. 2011) ("[A] request to preliminarily enjoin alleged trademark infringement is subject to traditional equitable principles."); Salinger v. Colting, 607 F.3d 68, 79–80 (2d Cir. 2010) ("[A district court must . . . consider whether [the plaintiff] is likely to suffer irreparable injury in the absence of an injunction, . . . balance the competing claims of injury, and . . . pay particular regard for the public consequences in employing the extraordinary remedy of injunction.") (quoting Winter v. Nat. Res. Def. Council, Inc., 555 U.S. 7, 22–24 (2008) (internal quotations omitted)).

134. *See* Visa IP Policy, *supra* note 110.

135. *See* Bridy, *Blockades*, *supra* note 8, at 1563 ("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.") (citing 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.")).

136. *See* Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U. L. REV. 1485, 1487 (2014).

137. Derek A. Dion, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash*, 2013 U. ILL. J.L. TECH. & POL'Y, 165, 167 (2013).

developing Bitcoin,[138] apparently developed the system in a decentralized fashion in part to insulate it against organized disruption like direct government interference.[139] Bitcoin is decentralized in a way that makes it difficult to find a central actor to coerce.

But it is not entirely clear that cryptocurrencies can cut out all need for reliance on middlemen. Indeed, Professor Bridy's solution may trade reliance on one intermediary for another. People who deal exclusively in Bitcoin need never exchange them for another currency, but many owners of Bitcoin will seek to exchange them at some point. Bitcoin exchanges convert Bitcoin to currencies like the U.S. Dollar at rates determined by the exchange.[140] Those exchanges provide a potential leverage point for regulatory activity or jawboning. Scholars have already identified potential regulatory interventions that could slow Bitcoin transactions.[141] IPEC or some other state actor could pressure an exchange to stop processing transactions for repeat infringers in exchange for not attempting regulatory intervention. Bitcoin exchanges may pursue their rational self-interest just like payment processors.[142] Exchanges might prefer to comply with soft coercion to avoid new legislation or regulation, just as payment processors found it reasonable to deal with IP owners rather than risk new legislation. Thus, vendors will only be insulated from the potential effects of jawboning if they opt entirely out of traditional payment systems. In addition, to the extent that Bitcoin and other decentralized currencies are viewed as means to illegal ends, they may be likely to attract regulatory attention.

Another limitation of cryptocurrencies is highlighted by the recent

---

138. *See* Bayern, *supra* note 136, at 1488. Nakamoto appears to be a pseudonym. *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 162 (2012).

139. *See* Posting of Satoshi Nakamoto to cryptography@metzdowd.com (Nov. 7, 2008), http://www.mail-archive.com/cryptography@metzdowd.com/msg09971.html ("Governments are good at cutting off the heads of a centrally controlled network[ ] like Napster, but pure [peer-to-peer] networks like Gnutella and Tor seem to be holding their own.").

140. *See* Notice of Filing of a Proposed Rule Change to BZX Rule 14.11(e)(4), Commodity-Based Trust Shares, To List and Trade Winklevoss Bitcoin Shares Issued by the Winklevoss Bitcoin Trust, 81 Fed. Reg. 45554 (proposed July 14, 2016). Bitcoin exchange rates have fluctuated widely, compared to traditional currency pairs. *See* Eric Engle, *Is Bitcoin Rat Poison? Cryptocurrency, Crime, and Counterfeiting (CCC)*, 16 J. HIGH TECH. L. 340, 341 n.5 (2016); Trevor I. Kiviat, Note, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 584 (2015).

141. Indeed, many scholars have analyzed whether Bitcoin exchanges are susceptible to regulation as financial institutions or securities traders. *See, e.g.*, Dion, *supra* note 137, at 197.

142. *Cf.* Bridy, *Scalability*, *supra* note 88, at 715–16 ("Forced to choose between protecting themselves from liability and protecting the expressive rights of their users, service providers [protected by the DMCA safe harbor] are much more likely to err on the side of caution.").

dissolution of Mt. Gox, once the world's largest Bitcoin exchange:[143] Sometimes, the middlemen are not reliable. Mt. Gox announced bankruptcy in 2014 after hackers apparently stole 850,000 Bitcoin valued at $460 million.[144] Consumers may hesitate to rely on a financial system subject to exploits like the Mt. Gox attack.[145] It's also not entirely clear that Bitcoin is immune to tampering.[146] In addition, Bitcoin is often used for illegal gambling, drug transactions, and donations to criminal hacker groups.[147] Customers looking for a legitimate experience and the security that comes with a major credit card may go elsewhere. To the extent that this is true, Bitcoin and other cryptocurrencies will provide limited utility for the average consumer, and thus of limited benefit to vendors hoping to avoid U.S. copyright and trademark law.

In fact, the use of Bitcoin or cryptocurrencies may well divide illicit from authentic actors. If vendors looking to avoid copyright liability use cryptocurrencies to avoid an uncomfortable conversation with online intermediaries, the method of avoidance will significantly cut into profits. Bitcoin's current level of adoption, for example, is low compared to the use of standard currencies,[148] but it may grow if the system finds ways to simplify transactions for unsophisticated users,[149] and provide fraud protection that is currently hard to replicate without trust intermediaries.

---

143. *See* Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014), https://www.wired.com/2014/03/bitcoin-exchange/.

144. *See id.*

145. That's not to say that financial institutions that deal in standard currencies like the dollar are immune to hacking, but mechanisms like the coverage provided by the Federal Deposit Insurance Corporation backstop those institutions against loss. *See* Sarah Gruber, Note, *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?*, 32 QUINNIPIAC L. REV. 135, 159–61 (2013) (explaining risks inherent in the Bitcoin system).

146. *See, e.g.*, Bayern, *supra* note 136, at 1490–91 (noting that while successful disruption by a single party is unlikely, disputes in the blockchain are resolved in favor of transactions backed by the most computing power, which leaves open the possibility that faster computers and specialized hardware might theoretically provide some level of effective "voting" power).

147. *See* Dion, *supra* note 137, at 169.

148. *See* Bridy, *Blockades*, *supra* note 8, at 1566; Michael Jackson, *Bitcoin's Big Challenge in 2016: Reaching 100 Million Users*, COINDESK (Jan. 1, 2016), http://www.coindesk.com/2016-bitcoin-challenge-100-million-users/ (reporting roughly 10 million Bitcoin wallets and roughly 200,000 Bitcoin transactions per day); *How Many People Really Own Bitcoin—and Why Does it Matter?*, BITSCAN (Feb. 10, 2014), http://bitscan.com/bitnews/item/how-many-people-really-own-bitcoins-and-why-does-it-matter (as of late 2014, 31 million transactions had taken place throughout Bitcoin's history, and roughly 250,000 addresses held more than a fractional amount of Bitcoin).

149. *See* Jackson, *supra* note 148.

CONCLUSION

Professor Bridy's article highlights the political economy of jawboning, the pressure it puts on payment processors to carry water for IP owners, and the potential dangers jawboning poses for the continued viability of the territorial boundaries of copyright and trademark law. Turning to Bitcoin and other cryptocurrencies will provide avenues for vendors to service tech-savvy consumers unconcerned about Bitcoin's reputation as an illicit currency and willing to overlook risk of fraud. But that turn may not provide vendors with enough traffic to avoid dealing with payment processors.

The decision of payment processors to implement the best practices agreement may nevertheless provide vendors with some room to maneuver, at least to the extent that payment processors have preserved some discretion in implementing the agreement as they see fit, and so long as they do not all adopt the same terms. The procedure provided by payment processors is imperfectly disclosed. But given what we know, they outline a valid attempt to ensure that complaining owners have authentic rights, that alleged repeat infringers engage in chronic infringement, and that there is no "genuine issue" regarding the lawfulness of the merchant's sale of alleged infringing goods.