


2017

## PayPal is New Money: Extending Secondary Copyright Liability Safe Harbors to Online Payment Processors

Erika Douglas

Follow this and additional works at: <https://repository.law.umich.edu/mttlr>

 Part of the [Commercial Law Commons](#), [Intellectual Property Law Commons](#), [Internet Law Commons](#), and the [Legislation Commons](#)

---

### Recommended Citation

Erika Douglas, *PayPal is New Money: Extending Secondary Copyright Liability Safe Harbors to Online Payment Processors*, 24 MICH. TELECOMM. & TECH. L. REV. 45 (2017).

Available at: <https://repository.law.umich.edu/mttlr/vol24/iss1/3>

This Article is brought to you for free and open access by the Journals at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Telecommunications and Technology Law Review by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact [mlaw.repository@umich.edu](mailto:mlaw.repository@umich.edu).

# **PAYPAL IS NEW MONEY: EXTENDING SECONDARY COPYRIGHT LIABILITY SAFE HARBORS TO ONLINE PAYMENT PROCESSORS**

*Erika Douglas\**

Cite as: Erika Douglas,

*PayPal is New Money: Extending Secondary Copyright Liability Safe Harbors to Online Payment Processors,*

24 MICH. TELECOM. & TECH. L. REV. 45 (2017).

*This manuscript may be accessed online at [repository.law.umich.edu](http://repository.law.umich.edu).*

## ABSTRACT

*The Digital Millennium Copyright Act (DMCA) has shaped the Internet as we know it. This legislation shields online service providers from secondary copyright infringement liability in exchange for takedown of infringing content of their users. Yet online payment processors, the backbone of \$300 billion in U.S. e-commerce, are completely outside of the DMCA's protection. This Article uses PayPal, the most popular online payment company in the U.S., to illustrate the growing risk of secondary liability for payment processors. First it looks at jurisprudence that expands secondary copyright liability online, and explains how it might be applied to PayPal. Then it considers legislative proposals and industry-self regulation that similarly target an increasing role for payment processors in the fight against online infringement. It argues that the introduction of a DMCA-like safe harbor for online payment processors offers a fairer and more efficient option for all stakeholders than the status quo of gradually expanding liability risk. It concludes with a discussion of important initial considerations in the design of such a safe harbor.*

---

\* LL.M., Stanford Law School, J.D. Western University. Thank you to Daphne Keller, Mark Lemley, George Addy and Matthew Gasperetti for their thoughtful input on the early drafts of this paper. All errors and omissions are my own. The title of this article is based on PayPal's 2016 Super Bowl advertisement promoting the company as the future of money, in contrast with stodgy images of "old money" fiat currency systems, see [https://www.youtube.com/watch?v=1dF9t\\_xQGks](https://www.youtube.com/watch?v=1dF9t_xQGks).

## TABLE OF CONTENTS

INTRODUCTION .....	46
A. <i>Background: E-commerce, PayPal, and Online Intermediary Safe Harbors</i> .....	48
B. <i>The Current Immunity Scheme for Online Intermediaries</i> .....	50
I. ONLINE PAYMENT PROCESSORS AT RISK: JURISPRUDENCE ON SECONDARY COPYRIGHT INFRINGEMENT, PROPOSED LEGISLATION, AND “VOLUNTARY” INDUSTRY REGULATION ..	52
A. <i>Secondary Copyright Infringement Liability Expands</i> ...	52
B. <i>Secondary Copyright Infringement Liability and Visa</i> ..	54
1. <i>Contributory Copyright Infringement in Visa</i> .....	54
2. <i>Vicarious Copyright Infringement in Visa</i> .....	64
3. <i>Applying Secondary Copyright Infringement Analysis to PayPal</i> .....	67
B. <i>Legislative Leanings Toward Payment Processor Enforcement Online</i> .....	74
C. <i>Payment Processors “Voluntarily” Police Copyright Infringement</i> .....	78
1. <i>The Payment Processor Agreement: Few Merchant Rights, Weak Payment Processor Liability Protections</i> .....	78
2. <i>Unilateral Denials of Service by Payment Processors</i> .....	83
II. EVALUATING OPTIONS FOR THE LEGAL TREATMENT OF ONLINE PAYMENT PROCESSORS: EFFICIENCY AND FAIRNESS CONSIDERATIONS .....	85
III. INITIAL CONSIDERATIONS IN THE DESIGN OF AN ONLINE PAYMENT PROCESSOR SAFE HARBOR FOR THE FUTURE.....	90
CONCLUSION .....	93

## INTRODUCTION

The Digital Millennium Copyright Act (DMCA) provides online intermediaries with a liability shield from the copyright infringement of their users, provided certain conditions are met.<sup>1</sup> Congress made clear that the DMCA’s purpose was to foster the robust expansion of electronic commerce in two ways: (1) by reducing the legal uncertainties of conducting business online and (2) by creating mechanisms to combat online infringement.<sup>2</sup> The legislation was designed to allay the fears of copyright holders about their works being made available online, where unauthorized copies proliferate with unprecedented ease. Given the focus on promoting commerce online, it seems odd that payment processors—the lynchpins of all electronic commerce—are not within the protection of the DMCA. Granting such protec-

---

1. 17 U.S.C. § 512 (2012).

2. S. Rep. No. 105–190, at 2 (1998).

tion would certainly have contributed to the congressional goal of creating “a thriving electronic marketplace” for intellectual property works online.<sup>3</sup>

One possible explanation for the omission is that Congress did not have payment processors in mind when the DMCA was passed. PayPal—now the most popular online payment service provider in the U.S.—was founded in 1998, coincidentally the same year the DMCA was enacted. But credit card companies had been offering online payment processing for several years by then, with the first online payments occurring around 1994.<sup>4</sup> By 1996 an estimated \$500-600 million in online transactions were being processed,<sup>5</sup> almost all of which were credit card payments.<sup>6</sup> This growth was sufficiently rapid that Congress would have been aware of the technology and its relevance to e-commerce. Although online payments were relatively new, it is conceivable that a future-oriented law, such as the DMCA, might have incorporated protection for online payment processors at the time it was passed.

A more likely explanation for the omission of payment processors from the DMCA safe harbor is that Congress never foresaw secondary liability extending to such intermediaries.<sup>7</sup> In 1998, secondary copyright infringement litigation had yet to name any payment processors as defendants. Theories of secondary copyright infringement were significantly more circumscribed and, as this Article explains, expanded in scope only after the DMCA was passed.

Reconsideration of a safe harbor for payment processors is timely, given the growing scope of liability for secondary copyright infringement. In fact, the U.S. Copyright Office is in the midst of a public study looking at the impact and effectiveness of the DMCA safe harbor provisions.<sup>8</sup> One question posed by the study is whether courts have properly construed the entities and activities covered by the Section 512 safe harbors.<sup>9</sup> This relates to

---

3. H.R. Rep. No. 105–551, pt. 1, at 9 (1998).

4. See Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523 n.103 (2015); see also Michael Grothaus, *You’ll Never Guess What The First Thing Ever Sold On The Internet Was*, FAST COMPANY, Nov. 26, 2015, <https://www.fastcompany.com/3054025/fast-feed/youll-never-guess-what-the-first-thing-ever-sold-on-the-internet-was>.

5. Christopher Anderson, *In Search of the Perfect Market*, THE ECONOMIST, May 8 1997, <http://www.economist.com/node/596262>.

6. Robert F. Stankey, *Internet Payment Systems: Legal Issues Facing Businesses, Consumers and Payment Service Providers*, 6 J. OF COMM. L. AND POL’Y 11, 12 (1998).

7. Bridy, *supra* note 4, at 1538–39.

8. Section 512 Study: Notice and Request for Public Comment, 80 Fed. Reg. 81,862 (Dec. 31, 2015); U.S. COPYRIGHT OFFICE, SECTION 512 STUDY, <https://www.copyright.gov/policy/section512/>; More broadly, the House Judiciary Committee recently concluded a review of copyright law to assess whether it is keeping pace with the digital age. Press Release, Chairman Bob Goodlatte, Chairman Goodlatte Announces Comprehensive Review of Copyright Law (Apr. 24, 2013) <https://judiciary.house.gov/press-release/chairmangoodlatteannouncescomprehensivereviewofcopyrightlaw/>.

9. Section 512 Study, *supra* note 8, at 81,868.

the broader question of whether our nation's copyright laws are keeping pace with the digital age, which Congress has been studying intently in recent years.<sup>10</sup>

This Article explains why online payment processors face increasing risk of secondary copyright liability. Then it considers whether DMCA-like safe harbors should be expanded to such intermediaries. PayPal is used as an example throughout the analysis because of its significant popularity and size—post eBay spinoff, PayPal is the fourth largest payment processor in the U.S., trailing only the major credit card companies.<sup>11</sup>

After a brief introductory section on e-commerce and the current DMCA safe harbor regime, Part I traces the expansion of secondary copyright liability to online intermediaries that are increasingly tangential to the direct infringement. It then applies the reasoning of the leading case on secondary liability of credit card companies for online infringement, *Perfect 10, Inc. v. Visa International Service, Ass'n*, to the business model of PayPal. The analysis suggests that online payment processors are at a higher risk for secondary copyright liability than traditional credit card companies, due to the differences in their business models. Finally, it examines broader trends, including recently proposed legislation and industry self-regulation, that also indicate increasing demands on payment processors to police online copyright infringement.

Part II looks at two major options for policy and lawmakers in relation to online payment processor liability: (1) continuing the current approach of industry self-regulation by payment processors and the slow evolution of common law liability risk or (2) intervening with the enactment of a DMCA-like liability safe harbor for some or all payment processors. It concludes that the statutory safe harbor is a fairer and more efficient option, remedying the risk of over-blocking of legitimate commerce that characterizes the *status quo*. Part III discusses important initial considerations in the design of such a copyright liability safe harbor for online payment processors.

#### A. Background: E-commerce, PayPal, and Online Intermediary Safe Harbors

Along with other key pieces of legislation passed in the 1990s, the DMCA is credited with creating a permissive online legal environment that made the U.S. a worldwide center for Internet innovation and online commerce. As one author explains, “[j]ust as nineteenth-century American

---

10. See, e.g., Congressional Hearings and Statements to Congress, U.S. COPYRIGHT OFFICE, <https://www.copyright.gov/laws/hearings> (last visited Oct. 15, 2017); U.S. Copyright Review, H. COMM. ON THE JUDICIARY, <http://judiciary.house.gov/index.cfm/us-copyright-law-review> (last visited Oct. 15, 2017).

11. Jim Daly, *Spinoff Ranks PayPal as Solid No. 4 Among Payments Companies by Market Cap*, DIGITAL TRANSACTIONS (Aug. 17, 2015), <http://www.digitaltransactions.net/spinoff-ranks-paypal-as-a-solid-no-4-among-payments-companies-by-market-cap/>.

judges altered the common law in order to subsidize industrial development, American judges and legislators altered the law at the turn of the Millennium to promote the development of Internet enterprise.”<sup>12</sup> Since the DMCA was enacted in 1998, online commerce has become an integral part of day-to-day life. In 1998, U.S. retail e-commerce sales were estimated at almost \$5 billion.<sup>13</sup> This rose exponentially to \$299 billion in 2014, the most recent Census Bureau estimate.<sup>14</sup>

The way customers make payments online is evolving quickly as well. In 2014, for the first time in global e-commerce, “alternative” payment methods overtook credit card payments as the preferred forms of payment.<sup>15</sup> Newer modalities, such as PayPal and Alipay, are displacing more traditional credit cards as the consumer’s choice for online payments to businesses and to peers. This shift toward alternative payment methods is expected to be most dramatic in North America,<sup>16</sup> which has lagged in adoption of alternative payments compared to that of other regions.

A corollary to this growth in e-commerce has been equal or greater growth in online intellectual property infringement. Digital works can be copied, distributed, and even sold with unprecedented ease. The amount of infringing material accessed via the Internet more than doubled from 2010 to 2012 alone.<sup>17</sup> An estimated one-quarter of all bandwidth on the Internet in North America, Europe, and Asia is devoted to hosting, sharing, and acquiring infringing material.<sup>18</sup> The flexibility and anonymity of online sales make it significantly harder to catch merchants engaging in such commerce. The rise of e-commerce has also facilitated global sales of physical products that infringe intellectual property rights. The estimated total value of counterfeit goods sold worldwide in 2015 was \$1.8 trillion (online and offline), and the

---

12. Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 668–69 (2014).

13. U.S. CENSUS BUREAU, 2015 ANNUAL RETAIL TRADE SURVEY: U.S. RETAIL TRADE SALES - TOTAL AND E-COMMERCE, <https://www.census.gov/retail/index.html> (2017); *Monthly & Annual Retail Trade: Definitions*, U.S. CENSUS BUREAU, <https://www.census.gov/retail/definitions.html> (last visited Oct. 15, 2017) (defining e-commerce to include sales of goods and services where the buyer places an order, or the price and terms of the sale are negotiated, over an Internet, mobile device, e-mail or other comparable online system; payment may or may not be made online).

14. *Id.*

15. *Global Payments Report Preview*, WORLDPAY, 5–7 (Nov. 2015), <http://offers.worldpayglobal.com/rs/850-JOA-856/images/GlobalPaymentsReportNov2015.pdf>. Alternative payments include all types of payment other than those run on global Visa, MasterCard or AmEx networks, but payment services like PayPal and Alipay account for a significant 20.5% overall. PayPal is included in the sub-category dubbed “ewallets.” It is not clear how the Worldpay report categorizes services where PayPal uses Visa and MasterCard networks as the underlying payment method.

16. *Id.* at 10.

17. Section 512 Study, *supra* note 8, at 81,862.

18. *Id.*

U.S. trade representative has predicted that online sales of pirated goods may exceed those in physical markets.<sup>19</sup>

The result is that copyright holders are clamoring for better solutions to enforce their rights online. Instead of chasing after each end user, which can be futile and costly, copyright holders are increasing efforts to vindicate their rights through or against online intermediaries. The past two decades have seen a “seismic shift” away from suing direct infringers toward suing indirect facilitators that have “less and less connection to the act of infringement.”<sup>20</sup> Online intermediaries who supply technology have increasingly been held liable for infringement by their users, at least when the DMCA does not apply. Payment processors are a prominent online intermediary in the facilitation of e-commerce, including transactions that involve intellectual property rights infringement, and appear to be a target of choice for rights enforcement. The question is whether online commerce will continue to thrive if payment processors become targets for secondary copyright infringement suits.

#### B. *The Current Immunity Scheme for Online Intermediaries*

The combination of two pieces of legislation, the DMCA and the Communications Decency Act (CDA), provide many online intermediaries in the U.S. with broad immunity from monetary damages related to their users’ acts online.<sup>21</sup> Section 230 of the CDA provides that intermediaries, such as Internet service providers (ISPs), are not considered the publishers or speakers of the content of their users.<sup>22</sup> This establishes broad immunity from causes of action attempting to hold such online intermediaries liable for information made available online by third parties. The CDA does not, however, provide immunity from intellectual property laws.<sup>23</sup>

This intellectual property “gap” in the CDA is filled by the DMCA. The DMCA provides broad immunity from user’s copyright infringement for much of the conduct of online service providers, provided certain conditions are met. The four types of activities protected from infringement liability are: (1) transmitting or routing the material of others over an online network (generally applicable to true “conduits,” such as Internet access providers); (2) temporarily storing or caching the material of others to be able to trans-

---

19. *Luxury goods: Counterfeit.com*, THE ECONOMIST (July 30, 2015), <https://www.economist.com/news/business/21660111-makers-expensive-bags-clothes-and-watches-are-fighting-fakery-courts-battle>.

20. Mark A. Lemley and R. Anthony Reese, *Reducing Digital Copyright Infringement without Restricting Innovation*, 56 STAN. L. REV. 1345, 1353 (2004).

21. Communications Decency Act, 47 U.S.C. § 230 (2006).

22. *Id.* §§ 230(c)(1), 230(e)(3) (stating that “[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,” and preempting any state law to the contrary).

23. *Id.* § 230(e)(2).

mit at a later time to other users; (3) storing information at the direction of an end user; and (4) operating information location tools that refer or link users to infringing online material (often applicable to search engines). Payment processors are not within the scope of these categories and have no protection from liability under the DMCA.<sup>24</sup>

The provisions applicable to search engines (“information location tools”) provide a good example of how the safe harbor operates.<sup>25</sup> To benefit from immunity, the search engine operator must either (1) have no actual knowledge or “aware[ness] of facts or circumstances from which infringing activity is apparent”—so called “red flag” knowledge—or (2) expeditiously remove or disable access to infringing material of which it knows or is aware.<sup>26</sup> In other words, if there is knowledge of infringement, the intermediary’s immunity is conditioned on its implementation of a notice and takedown regime that removes infringing content upon receipt of a DMCA-compliant notice from the copyright holder.<sup>27</sup> The theory behind placing the notice burden on rights holders is that “copyright holders know precisely what materials they own” and are therefore better positioned than intermediaries to efficiently determine what material is copyrighted and what is not.<sup>28</sup> The DMCA explicitly states that it imposes no affirmative duty on online service providers to investigate whether or not user content infringes copyright.<sup>29</sup>

There are other conditions that some online intermediaries must meet to qualify for the DMCA safe harbor: an agent must be delegated to receive notifications of infringement and a policy providing for termination of repeat infringers must be reasonably implemented.<sup>30</sup> Lastly, the intermediary may not receive “financial benefit directly attributable to the infringing activity” if they have the right and ability to control that activity.<sup>31</sup>

---

24. *Perfect 10, Inc. v. Visa Int’l Serv., Ass’n*, 494 F.3d 788 n.4 (9th Cir. 2007) (“Defendants are not ‘service providers’ within the scope of the DMCA, they are not eligible for these safe harbors.”).

25. Digital Millennium Copyright Act, 17 U.S.C. § 512(d).

26. *Id.* § 512 (d)(1)(A), (B) and (C).

27. The elements required in such a notification are set out in *Id.* § 512(c)(3).

28. *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1022 (9th Cir. 2013) (“Copyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers like Veoh, who cannot readily ascertain what material is copyrighted and what is not.”).

29. 17 U.S.C. § 512(m); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113–14 (9th Cir. 2007) (Section 512(c) “impose[s] no such investigative duties on service providers,” and “place[s] the burden of policing copyright infringement . . . squarely on the owners of the copyright”).

30. 17 U.S.C. § 512(i) (policy must “provide [. . .] for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers”); *see also Perfect 10*, 488 F.3d at 1109–111 (explaining what constitutes a “reasonably implemented policy”).

31. *E.g.* 17 U.S.C. § 512(e)(1)(B).



Overall, the DMCA creates an optional trade-off scheme for intermediaries; if the intermediary implements a reasonable content-takedown policy and meets the other requirements, they gain the safe harbor protection from liability for monetary and most equitable remedies arising from the copyright infringing content of others on their systems. Alternatively, the intermediary is free to ignore notice from rights holders and gamble on whether or not they will be found liable at common law for secondary copyright infringement.

I. ONLINE PAYMENT PROCESSORS AT RISK: JURISPRUDENCE ON  
SECONDARY COPYRIGHT INFRINGEMENT, PROPOSED LEGISLATION,  
AND “VOLUNTARY” INDUSTRY REGULATION

This Part traces the recent expansion of secondary copyright liability for online intermediaries. It then looks at the challenges this expansion raises for payment processors, using PayPal as an example and applying the reasoning of the leading case on secondary liability of credit card companies for online infringement, *Perfect 10, Inc. v. Visa International Service, Ass'n (Visa)*. It then examines proposed legislation targeting the same payment intermediaries and the industry self-regulation compromise that resulted. This brewing storm of legislative change and common law developments in payment processor intellectual property liability is well summarized by PayPal in its 2015 financial risk disclosure:<sup>32</sup>

Changes in law have increased the penalties for intermediaries providing payment services for certain illegal activities and additional payments-related proposals are under active consideration by government authorities. Intellectual property rights owners or government authorities may seek to bring legal action against providers of payments solutions, including PayPal, that are peripherally involved in the sale of infringing items.

A. *Secondary Copyright Infringement Liability Expands*

Secondary copyright infringement liability has been expanding since the late 1990s, as copyright holders try various approaches to enforce their rights against intermediaries.<sup>33</sup> These cases form the backdrop to many of the concepts discussed in *Visa*. In the first of a series of seminal cases, *For-*

---

32. PAYPAL INC., Form 10-K (2015), <https://investor.paypal-corp.com/secfiling.cfm?fileID=1633917-16-113&CIK=1633917>.

33. See e.g. John F. Blevins, *Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms*, 34 CARDOZO L. REV. 1821, 1821 (2013) (“Copyright owners, accordingly, are attempting to increase the breadth and expense of secondary copyright liability for Internet platforms by institutionalizing uncertainty within legal doctrine.”); See generally Lemley & Reese, *supra* note 20 (tracing the significant shift toward copyright holders suing “facilitators” of infringement, rather than end users).

*novisa, Inc. v. Cherry Auction Inc.*, the operator of a physical “swap meet” was held liable for the sale of infringing goods at his marketplace.<sup>34</sup> *Fonovisa* hinted at what was to come for online intermediaries in *A&M Records, Inc. v. Napster, Inc.*, where a similar theory was applied to find Napster liable.<sup>35</sup> Napster was an infamous operator of a centralized electronic file sharing system that was used predominantly to exchange unlicensed, copyrighted music files. The *Napster* and *Fonovisa* cases both interpreted vicarious copyright liability broadly, expanding the scope of what constitutes financial benefit and control, elements of secondary copyright infringement that are addressed in more detail below.<sup>36</sup>

Shortly thereafter, *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* and similar cases extended secondary copyright infringement liability to the distribution of software that enabled peer-to-peer exchange of copyrighted music.<sup>37</sup> Unlike Napster’s centralized file exchange, Grokster’s software was based on a distributed system of file searching and sharing. Grokster played no central role as intermediary, other than the initial software distribution, but it was still held liable. The Supreme Court revived the concept of “inducing” infringement, basing liability on the intent to induce infringement, despite the product being capable of substantial non-infringing use.<sup>38</sup> Some consider *Grokster*’s inducement theory to be a distinct category of secondary liability, while others see it as a subcategory of contributory copyright infringement.<sup>39</sup> Regardless of the categorization, *Grokster* significantly broad-

---

34. See generally *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir. 1996) (establishing that a copyright holder has an actionable claim).

35. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1022 (9th Cir. 2001) (finding “Napster provides ‘the site and facilities’ for direct infringement” and citing *Fonovisa*).

36. See Blevins, *supra* note 33, at 1846 (tracing the expansion of vicarious liability from a narrow, agency law related doctrine).

37. *Metro-Goldwyn-Mayer Studios v. Grokster, Ltd.*, 545 U.S. 913, 919–20 (2005) (“defendants . . . distribute free software products that allow computer users to share electronic files through peer-to-peer networks, so called because users’ computers communicate directly with each other, not through central servers”); see also *re Aimster Copyright Litigation*, 334 F.3d 643, 646 (7th Cir. 2003) (“copies of the songs reside on the computers of the users and not on Aimster’s own server. . .”).

38. *Grokster, Ltd.*, 545 U.S. at 935–37; see generally Debra R. Rydarowski, *The Tortious Beginnings of Contributory Copyright Infringement: The Concerted Action Key to Grokster*, 31 SETON HALL LEGIS. J. 215 (2006) (analyzing how Grokster and another respondent, StreamCast networks, Inc. faced litigation from rights holders, alleging contributory infringement and vicarious liability for the direct infringement committed by Grokster users).

39. Paul Goldstein, GOLDSTEIN ON COPYRIGHT, § 8.1.3 (3d ed. Supp. 2013) (describing contributory infringement as long including inducement as a “separate, but sometimes overlapping, ground for secondary liability”); Mark Bartholomew, *Copyright, Trademark and Secondary Liability after Grokster*, 32 COLUM. L.J. & ARTS 445, 465–66 (2009) (referring to *Grokster* as creating a new category of contributory copyright infringement liability); Sverker K. Hogberg, *The Search for Intent-Based Doctrines of Secondary Liability in Copyright Law*, 106 COLUM. L. REV. 909, 913 (2006) (“In declaring a new standard of “inducement” liability, the Court has made it clear that copyright law encompasses a separate, intent-based secondary liability doctrine.”).

ened the potential for secondary copyright infringement liability by reinvigorating the inducement grounds.

The series of cases against intermediaries such as Fonovisa, and file-sharing companies like Napster, Grokster, and others, have all resulted in findings of secondary copyright infringement by the intermediary for the copyright violations of the company's end users. They illustrate how secondary copyright liability is slowly expanding to reach "a wider array of defendants with increasingly tangential relationships to the direct infringer."<sup>40</sup>

### B. Secondary Copyright Infringement Liability and Visa

In 2007, credit card processors became the latest intermediary targeted by copyright holders in attempts to expand secondary copyright infringement liability. *Visa* involved third parties purchasing unlicensed copies of risqué photos in which the plaintiff, Perfect 10, held copyright.<sup>41</sup> The purchases were made online, in many cases using a Visa or MasterCard credit card. The Ninth Circuit found Visa and MasterCard were not liable for secondary copyright infringement under theories of contributory infringement or vicarious infringement.

The following section considers the analysis of each of these types of secondary copyright infringement in *Visa*, along with a recent case that adopted the dissenting approach from *Visa*, *Gucci Am., Inc. v. Frontline Processing Corp. (Gucci)*.<sup>42</sup> It then analyzes how each theory of liability might be applied to PayPal to highlight potential differences in the analysis between traditional credit card companies and the newer generation of online payment processors.

#### 1. Contributory Copyright Infringement in *Visa*

*Visa* synthesizes recent cases to describe contributory copyright infringement liability as requiring (1) knowledge of another's infringing conduct and (2) either material contribution to, or inducement of, the direct infringement.<sup>43</sup> This analytical structure was applied to Visa and MasterCard's conduct, but their role was too attenuated for liability. However, the dissenting opinion in *Visa*, and the *Gucci* decision that followed that dissent would have held Visa and MasterCard contributorily liable.

---

40. Batholomew, *supra* note 39, at 445.

41. *Visa*, 494 F.3d at 793.

42. *Gucci Am., Inc. v. Frontline Processing Corp.*, 721 F. Supp. 2d 228, 252–53 (S.D.N.Y. 2010).

43. *Visa*, 494 F.3d at 795; *see also* 17 U.S.C. § 101; *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (citing *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir.1971)).

a. Material Contribution: The *Visa* Dissent Lives On

In determining whether there was a material contribution by the credit card companies to the copyright infringement of their customers, the *Visa* majority focuses on a “site and facilities” theory. This theory—which originated with in *Fonovisa* and was then applied in *Napster*—imposes liability on defendants who supply a physical or virtual “centralized place” where infringing works can be “collected, sorted, found and bought, sold or exchanged.”<sup>44</sup> The provision of this centralized site is sufficient to establish a material contribution to liability when the defendant “actively strives to provide the environment and the market for counterfeit . . . sales to thrive.”<sup>45</sup> The majority in *Visa* concludes that the payment processors have not created any such site where infringing activity occurs, and the court identifies this as a key distinction from the prior cases where liability was imposed.

The majority’s position is also rooted in its separation of the act of payment and from the infringing acts online. It reasons that the infringing act of “reproduction, alteration, display, and distribution” of the disputed photos online is separate from the act of payment for copies of such photos. Although the majority concedes that payment systems make it easier to profit from infringement, they reason the payment processor’s contribution does not reach the threshold of materiality because infringement could occur online even if the defendants did not use the credit card payment system. The infringing images would still be displayed on unauthorized websites absent payment. The majority distinguishes past cases in which intermediaries were held liable, finding the likes of *Fonovisa*, *Napster*, and *Grokster* all played more integral location and distribution roles than *Visa* or *MasterCard*.<sup>46</sup>

Judge Kozinski takes issue with this distinction in a strongly worded dissent. He emphasizes that online payment is *not* separable from the act of infringement as the majority claims. First, he points out that the plaintiff, *Perfect 10*, claims the infringement is “by sale” of the copyrighted images, making it impossible to separate that sale from the infringing acts of “reproduction, alteration, display or distribution,” as the majority does.<sup>47</sup> Second, he argues the majority’s position is inconsistent with *Perfect 10 Inc. v. Amazon.com, Inc. (Amazon)*,<sup>48</sup> in which the court found Google’s search engine materially contributed to copyright infringement when it was used to help find infringing images, even though this was also *not* an act of reproduction, alteration, display or distribution. Judge Kozinski concludes that “distribu-

---

44. *Visa*, 494 F.3d at 799.

45. *Fonovisa, Inc.*, 76 F.3d at 264.

46. *Visa*, 494 F.3d at 796.

47. *Id.* at 814 (Kozinski, J., dissenting).

48. *Perfect 10, Inc. v. Amazon.com*, 487 F.3d 701, 729 (9th Cir. 2007) Although there was a finding of contributory infringement in *Amazon*, Google’s conduct was ultimately found likely to constitute fair use.

tion and payment are . . . like love and marriage—you can't have one without the other."<sup>49</sup>

Judge Kozinski then goes on to reject the majority's attempt to distinguish search services in *Amazon* from payment services in *Visa* based on the availability of alternatives. The majority argues infringement could continue even absent credit card payments because of "other viable funding mechanisms," which make the payment services non-material to infringement.<sup>50</sup> Judge Kozinski observes that if the availability of alternatives determined materiality, the correct position would have been to find materiality for the credit card defendants in *Visa* but not for Google in *Amazon*.<sup>51</sup> There are a wide variety of alternatives to Google for locating infringing images on the web, including the multitude of other search engines, e-mails, online chat, messages on discussion forums, or peer-to-peer networking, yet Google was found to have materially contributed to infringement.<sup>52</sup> In contrast, substitutes for credit cards in online payment at the time of *Visa* were almost nonexistent. Judge Kozinski summarizes his position by noting "[i]f it mattered whether search engines or credit cards were more important to peddling infringing content on the Internet, the cards would win hands down."<sup>53</sup>

In Judge Kozinski's dissent, he argues the better approach to analyzing materiality is not to look at alternatives but instead to consider whether the action by the intermediary "substantially assists" in the infringement.<sup>54</sup> As in *Amazon*, Judge Kozinski would impose liability when a party has knowledge that infringing content was made available using their tools and "could take simple measures to prevent further damage" to the copyrighted works but fails to do so.<sup>55</sup> He finds this test is easily met in *Visa*, where the defendants "know about the infringements; they profit from them; they are intimately and causally involved in a vast number of infringing transactions that could not be consummated if they refused to process the payments; they have ready means to stop the infringements."<sup>56</sup>

---

49. *Visa*, 494 F.3d at 818.

50. *Id.* at 797.

51. *Id.* at 813 (Kozinski, J., dissenting) ("If the test for contributory infringement really were whether 'infringement could continue on a large scale [without the aid of the defendant] because other viable funding mechanisms are available', *Amazon* should have absolved Google of liability because of the availability of such obvious alternatives. But *Amazon* held that Google *could* be liable for contributory infringement because it 'substantially assists' users in finding infringing materials; the existence of other means of infringement was not even considered because no case has suggested this to be a relevant consideration.") (quoting the *Visa* majority).

52. *Id.* at 812–13.

53. *Id.* at 814.

54. *Id.*

55. *Id.* at 811 (quoting *Amazon, Inc.*, 487 F.3d at 729).

56. *Id.* at 816.

Judge Kozinski's dissent was picked up in a 2010 trademark infringement case, *Gucci*.<sup>57</sup> In this preliminary ruling, the Southern District of New York allowed the luxury brand's claims of contributory trademark infringement to proceed, but not their vicarious trademark infringement claims.<sup>58</sup> The defendants were three payment processors who provided their services to the operator of TheBagAddiction.com, a website devoted to selling counterfeit purses. Durango, one of the defendant payment processors, acted as a middleman to connect merchants like TheBagAddiction.com's owners with payment processors who in turn issued credit card merchant accounts. The two other defendants, Frontline and Woodforest, provided card processing services and banking services, respectively, to the website operator.

Throughout the decision, Judge Baer relies on Judge Kozinski's strongly worded dissent from *Visa*. He finds plausible claims of contributory trademark infringement based on "direct control and monitoring of the instrumentality used by a third party to infringe the plaintiff's mark," as well as a strong inference of knowledge or willful blindness as to the direct infringement.<sup>59</sup> This analysis reflects a difference between contributory infringement in trademark and copyright; in copyright, control is an element of vicarious rather than contributory infringement. Woodforest and Frontline were both found to have plausible control and knowledge of the trademark violations by TheBagAddiction.com.

Judge Baer distinguishes the *Visa* majority based on whether the payment was "an essential step in the infringement process."<sup>60</sup> In *Visa*, the infringement itself occurred online, so the majority differentiated between the act of credit card payment and the separate act of the website continuing to post infringing content without any payment. The credit card service providers lacked control, since they had no ability to remove or directly stop distribution of images online. In contrast, in *Gucci*, the physical shipment of goods did not occur until the credit card approval was obtained. Judge Baer found that for physical shipments of goods "it is not possible to distribute by sale without receiving compensation, so payment is in fact part of the infringement process."<sup>61</sup> Frontline and Woodforest plausibly had control because the goods would not be shipped without approval of payment from their credit card services. Judge Baer found the website was "functionally dependent" on the credit card processing to sell the goods, despite potential online payment alternatives, and this constituted sufficient control to plausibly allege contributory trademark infringement.<sup>62</sup> Judge Baer found Du-

---

57. *Gucci Am., Inc.*, 721 F. Supp. 2d at 252 n.9.

58. *Id.* at 246 (denying the motion to dismiss by the defendants). There were no subsequent proceedings.

59. *Id.* at 249, 253 (quoting *Visa*, 494 F.3d at 807 (Kozinski, J., dissenting)).

60. *Id.* at 252 (quoting *Visa*, 494 F.3d at 811–12 (Kozinski, J., dissenting)).

61. *Id.* at 253 (quoting *Visa*, 494 F.3d at 814 (Kozinski, J., dissenting)).

62. *Id.* at 253.

rango's middleman role of recruiting merchants provided insufficient control over the sale of infringing products on the website to establish contributory liability.<sup>63</sup>

The *Gucci* case must be taken with a grain of salt, as it was a preliminary motion to dismiss and there were no further proceedings. It is also a decision in trademark law, rather than copyright, leading to some differences in the legal analysis. The reasoning in the case is vague as to the distinction being made between the different actors—Frontline and Woodforest are found to have control and knowledge, but Durango is found to lack sufficient control, yet to have plausibly induced infringement.<sup>64</sup> Despite these caveats, the case remains of interest because it takes up the gauntlet of Judge Kozinski's well-argued *Visa* dissent. *Gucci* inches the law toward recognition of secondary copyright infringement liability for payment processors, in particular for processors that are not the major credit card companies protected by the *Visa* majority.

#### b. Knowledge of Direct Infringement

The second element of contributory copyright infringement is knowledge of the conduct that constitutes direct infringement. *Visa* did not address the knowledge element on the basis that the first element of material contribution was not met. The dissenting opinion in *Visa* mentions at one point that the defendants know of the infringement, but does not elaborate on how or why they have such knowledge.<sup>65</sup> Since *Visa* provides little insight on the knowledge element, the DMCA and other cases are discussed here to elaborate on the concept. Overall, knowledge has been a challenging concept for the courts and its boundaries have not been clearly defined in the online context.

The knowledge element is objective and is met by actual knowledge or by imputed constructive knowledge based on awareness of facts or circumstances from which infringing activity is objectively apparent. For either type of knowledge, a generalized awareness of the potential for direct in-

---

63. *Id.* at 251 (finding a failure to prove control by Durango). *See also id.* at 249 (finding a "strong inference" that all three defendants knew the owner of the counterfeit website traded in counterfeit products or were willfully blind to that fact). However, Durango satisfied the knowledge requirement and was found to potentially have induced infringement, as discussed below.

64. *Id.* *Gucci* also argued the payment processor and the bank had induced infringement. Both allegedly also advertised for high-risk merchants, but the conduct was less involved than Durango's actions. The court finds their conduct insufficient to plausibly plead an inducement claim, but no further reasoning is provided. The claims for contributory trademark infringement were allowed to proceed.

65. *Visa*, 494 F.3d at 810 (Kozinski, J. dissenting) (The defendants "know about the infringements; they profit from them").

fringement is not sufficient.<sup>66</sup> In *Napster*, for example, the court made clear that “evidence of actual knowledge of specific acts of infringement” is required for secondary copyright infringement.<sup>67</sup> In *Grokster*, the court clarified that “mere knowledge of infringing potential or of actual infringing uses would not be enough . . . to subject a distributor to liability.”<sup>68</sup>

The DMCA safe harbor provisions also reference knowledge requirements; actual or “red flag” constructive knowledge of infringing conduct can disqualify intermediaries from the liability safe harbors.<sup>69</sup> Some cases treat the elements that disqualify an intermediary from the safe harbor—such as financial benefit and the right and ability to control—as being identical to the parallel elements of claims for contributory infringement and vicarious liability.<sup>70</sup> Under this interpretation, the DMCA provides protection only from direct infringement, because the establishment of secondary infringement also establishes elements such as knowledge that disqualify service providers from the safe harbors.

The stronger argument is that the DMCA requires a higher degree of knowledge than the “knowledge” that must be shown for contributory infringement liability.<sup>71</sup> In other words, “knowledge” sufficient to prove contributory infringement liability would not preclude the intermediary from being protected by the DMCA safe harbors.<sup>72</sup> From the outset, Congress made clear that the DCMA’s knowledge standard was intended to be distinct from existing contributory-liability concepts.<sup>73</sup> This interpretation is more logical, because the DMCA was designed to provide liability protections for online intermediaries. It is highly unlikely that an intermediary would be

---

66. See, e.g., *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 439 (1984) (general knowledge that VCRs may be used for infringement is not sufficient for secondary copyright infringement liability as VCRs also have substantial non-infringing uses); *Tiffany (NJ) Inc. v. Ebay Inc.*, 600 F.3d 93, 107 (2d Cir. 2010) (discussing willful blindness in the context of the similar requirement for contributory trademark infringement, finding although eBay “clearly possessed general knowledge as to counterfeiting on its website” that generalized knowledge was insufficient to constitute “knowledge or reason to know” of trademark infringement by third parties).

67. *A&M Records Inc.*, 239 F.3d at 1021.

68. *Grokster, Ltd.*, 545 U.S. at 937.

69. 17 U.S.C. § 512(c)(1)(A)(i)–(ii), (d)(1)(A)–(B).

70. See, e.g., *In re Aimster Copyright Litig.*, 334 F.3d 643 (7th Cir. 2003).

71. See Goldstein, *supra* note 39 at § 8.3.2; see also *Perfect 10, Inc.*, 488 F.3d at 1114–15 (finding that although the defendant was aware of the activity occurring, it was not necessarily aware that the activity infringed copyright).

72. See R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability*, 32 Col. J.L. 427, 433–438 (2009) (discussion of the distinction between knowledge under the DMCA compared to contributory copyright infringement).

73. H.R. REP. NO. 105–551, pt.1, at 25 (1998) (“Once a provider becomes aware of a red flag, however, it ceases to qualify for the exemption [under the DMCA]. This standard differs from existing law, under which a defendant may be liable for contributory infringement if it knows or should have known that material was infringing.”).



found directly liable for the infringing conduct of their users, so protection from direct-infringement liability is not particularly useful. The utility of the DMCA protections is that they shield intermediaries from the more plausible risk of secondary-infringement liability.<sup>74</sup> Cases in the DMCA context have confirmed this, holding that even where there is fairly extensive factual knowledge of infringing conduct, the safe harbors still apply. For example, in one case involving the DMCA, e-mails to the intermediary's executives describing specific infringing content did not constitute sufficient knowledge to deny the DMCA protections.<sup>75</sup> In another, the knowledge that a high percentage of overall video streaming was infringing was insufficient to find "knowledge" that defeated the DMCA protections.<sup>76</sup>

This distinction in the level of knowledge is also evident in the DMCA notice system. When proper notice is provided, this is powerful evidence of knowledge, and unless the content is removed or blocked, causes the intermediary to lose the benefit of the DMCA safe harbor. But the DMCA's notice requirements are stringent and formal, and when they are not met there is no obligation for the intermediary to act. Non-compliant attempts at notice have been found insufficient even to prove red-flag knowledge of users' infringement.<sup>77</sup> In contrast, the sources of knowledge for contributory infringement may be much more widely drawn, with no specific form or content requirements for a finding of knowledge.<sup>78</sup> These differences result in a higher bar to show "knowledge" sufficient to preclude the application of DMCA safe harbors than for a finding of contributory copyright infringement.

Conversely, the differences outlined above are a reminder that when the DMCA is not at issue, the bar for finding the requisite knowledge may be lower. The *Gucci* case, which did not involve the DMCA, provides an example where knowledge of trademark infringement by payment processors was found plausible. Both of the payment processors for which knowledge was found had also investigated "chargebacks" from Visa and MasterCard for

---

74. See, e.g., Jonathan Band & Matthew Schruers, *Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act*, 20 CARDOZO ARTS & ENT. L. J. 295, 305 (2002).

75. See *UMG Recordings, Inc.*, 718 F.3d 1006 (stating that direct e-mails to executives about specific infringing content and third-party communications about material on the impugned site does not constitute "red flag" knowledge).

76. *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 32–35 (2d Cir. 2012) (stating that the generalized knowledge that "75–80% of all YouTube streams contained copyrighted material. . . [and an] estimated . . . 60% of YouTube's content was 'premium' copyrighted content—and that only 10% of the premium content was authorized" was not sufficient to find knowledge of infringement under the DMCA, although the question of whether this constituted willful blindness was remanded to the District Court).

77. *Corbis Corp. v. Amazon.com*, 351 F. Supp. 2d 1090, 1108–09 (W.D. Wash. 2004) (finding notices provided by other copyright holders to Amazon were not sufficient to show Amazon had red flag knowledge of the infringement of Corbis's rights).

78. Goldstein, *supra* note 39, at § 8.1.3.

counterfeit item purchases. The chargebacks occurred when customers disputed the charges on their credit card. The investigations meant the payment processors had received supporting documentation that described the counterfeit item purchased and the customer's complaint that the item was not genuine. The chargeback documentation also included the price, which Gucci argued was obviously not commensurate with genuine Gucci products and therefore signaled to the payment processors that there was infringement. In addition, one of the payment processors had reviewed the counterfeiter's business operations as part of its initial decision to provide payment services. This included multiple levels of review by the payment processor's employees, who looked at the website and its descriptions of counterfeit items. The finding of knowledge in *Gucci* was not, however, cabined to the specific knowledge of the transactions that were charged back. Instead, the chargebacks and business review plausibly supported overall knowledge or conscious avoidance of knowledge by the payment processors of the counterfeit product sales.

The *Gucci* case did not proceed to a full hearing on the merits. If it had, it may have been difficult to reconcile the finding of knowledge with another secondary trademark infringement case decided the same year, *Tiffany v. eBay Inc.*<sup>79</sup> The Tiffany jewelry company claimed eBay was contributorily liable for sales of counterfeit products by merchants on eBay's website. No knowledge was found, despite end consumer complaints to eBay about counterfeit Tiffany items similar to the chargebacks in *Gucci*. The plaintiff had sent multiple demand letters claiming at a general level that infringement was occurring and made thousands of filings to eBay indicating specific listings were counterfeit. Since eBay had removed the specific listings and suspended repeat offenders, any knowledge on eBay's part was not specific enough to show it knew or had reason to know counterfeit Tiffany goods were still being sold. The most significant factual difference from *Gucci* is that eBay did not review the merchant's business before services were offered (or at least such a review was not mentioned). This speaks to why payment processors may be at a greater risk for knowledge; the nature of their business often requires some diligence on the customer before services can be extended, creating the potential for arguments that the payment processor knew of the merchant's infringing business.

*Gucci* also highlights a factor that will continue to influence the knowledge of online payment processors. Thanks to developing technology for policing transactions, it is becoming more feasible for payment processors to know about substance of their customers' transactions. While some online intermediaries, like ISPs, transfer actual content, payment processors move only funds. In the past, this could have been an advantage in arguing against liability based on lack of knowledge; payment processors could be expected

---

79. *Tiffany (NJ) Inc.*, 600 F.3d at 96.

to have less knowledge about the legality of the items purchased in the transactions processed than intermediaries who processed infringing content. Now, the argument has less strength. Online gambling, online pharmacies, and online cigarette sales are all subject to payment processing restrictions based on the type of transaction.<sup>80</sup> For example, payment processors are required to identify and block illegal-gambling transactions under the regulations of the *Unlawful Internet Gaming Enforcement Act*.<sup>81</sup> Even before this legislation was passed, credit card networks used a coding/blocking system that relied upon a merchant's self-identified category code, "7995," for gambling, to impose geographic prohibitions on gambling transactions in order to comply with local laws.<sup>82</sup> To date, such knowledge is still too general for contributory infringement liability, but it is becoming more and more technologically feasible for payment processors to determine the nature of payments on their networks. For example, one can imagine further advancement of existing technology restricting online pharmacy purchases to identify the drugs by brand and the merchant to flag unauthorized sellers. The ironic result may be that as payment processors advance technology to better comply with laws, they may also be increasing their risk of claims they "know" about infringing transactions. Over the long term, a collision course is emerging as payment processors gain more knowledge about merchant transactions, while cases like *Gucci* chip away at the specificity of knowledge required for secondary infringement liability. Online payment intermediaries are left in the middle, in an increasingly precarious position, at risk for secondary copyright infringement claims.

### c. Inducement to Infringe Copyright in *Visa*

Some consider inducement of copyright infringement to be a distinct category of secondary liability, while others see it as a subcategory of contributory infringement.<sup>83</sup> The *Visa* case looked at inducement as an alterna-

---

80. See David Haskel, *A Good Value Chain Gone Bad: Indirect Copyright Liability in Perfect 10 v. Visa*, 23 BERKELEY TECH L. J. 405, 432–33 (2008) (showing cooperation between credit card companies and government agencies to fight against websites selling infringing or illegal content).

81. 31 U.S.C. §§ 5361–5367 (2012) (showing legislation that was directed at enforcement of state and federal gambling laws, which varied by jurisdiction and were being evaded by users through the use of online casinos).

82. Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L. J. 1037, 1061–63 (2010).

83. See, e.g., Paul Goldstein, *supra* note 39, § 8.1.3 (describing contributory infringement as long including inducement as a "separate, but sometimes overlapping, ground for secondary liability"); Mark Bartholomew, *Copyright, Trademark and Secondary Liability after Grokster*, 32 COLUM. L.J. & ARTS 445, 466 (2009) (referring to *Grokster* as creating a new category of contributory copyright infringement liability); Sverker K. Hogberg, *The Search for Intent-Based Doctrines of Secondary Liability in Copyright Law*, 106 COLUM. L. REV. 909, 913 (2006) ("In declaring a new standard of 'inducement' liability, the Court has made it clear that copyright law encompasses a separate, intent-based secondary liability doctrine.").

tive to material contribution, which, if met in conjunction with the knowledge requirement, establishes contributory copyright infringement.

*Grokster* revived the inducement branch of liability and expanded the potential for secondary copyright infringement liability by holding that “one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.”<sup>84</sup> *Grokster* explained that the critical element of inducement is the communication of an inducing message to users, which classically involves “advertising or solicitation . . . designed to encourage violations.”<sup>85</sup> In *Grokster*, the court found actual evidence of intent to induce infringement because the respondent (1) made efforts to serve former Napster users, who were known to infringe copyright; (2) had the principal object of their software being used to download copyrighted works, because their advertising profits increased with the use of the software for downloads; and (3) failed to develop filtering tools to try and control copyrighted content.<sup>86</sup>

The relevant question for inducement liability in *Visa* was whether Visa and MasterCard created or promoted their payment services *as a means of infringing copyright*. The defendants clearly promoted the use of their cards to pay for goods online, but the *Visa* majority distinguishes the defendants’ general marketing of their cards from promotion of the specific goods being purchased. While Napster and Grokster created and promoted their software systems explicitly for the purpose of facilitating music piracy and promoted them as such, Visa and MasterCard were not promoting their system as a means of breaking laws, nor were they designed to do so.

As with the analysis of “material contribution,” the majority continues to distinguish the less culpable act of facilitating payment processing from systems online that enable copying, altering, distributing, or displaying infringing material, or even locating, viewing or downloading infringing images. The infringing content, the majority reasons, is not available merely from the system of payment processing. Ultimately, the majority concludes that the conduct in *Grokster* and similar cases is distinguishable because the defendants did not engage in an affirmative act or clear expression of an intent to induce infringement.

Contrast this with the later *Gucci* case, where the defendant Durango’s marketing efforts crossed the line into plausible inducement of trademark infringement.<sup>87</sup> Durango acted as a middleman between merchants and payment processors to set up accounts. The company’s website marketed services specifically to “high risk merchant accounts” selling “replica”

---

84. *Grokster, Ltd.*, 545 U.S. at 919.

85. *Id.* at 937.

86. *Id.* 925–27.

87. *Gucci Am., Inc.*, 721 F. Supp. 2d at 248.

products.<sup>88</sup> Durango had also affirmatively acted to help the owner of TheBagAddiction.com in efforts to reduce chargebacks from customer complaints by designing a consent check box for the infringing website that required customers to acknowledge they were purchasing a “replica.” The court found this to be a plausible affirmative step taken to foster infringement—or in the alternative that Durango promoted its payment system as a means to infringe—and refused to dismiss the claim of inducement to infringement.<sup>89</sup> The other two payment processor defendants, although they allegedly advertised for “high risk merchants,” were found not to have taken sufficient affirmative steps to induce infringement. The court is not clear on whether the inducement claims against Durango could have proceeded if it simply advertised to high-risk merchant accounts without providing the check-box assistance aimed at avoiding customer chargebacks.

## 2. Vicarious Copyright Infringement in *Visa*

The final type of secondary infringement considered by *Visa* is vicarious copyright infringement. A defendant is liable for vicarious copyright infringement if he or she has (1) the right and ability to control or supervise the infringing conduct and (2) a direct financial interest in the infringing activity.<sup>90</sup> Unlike for contributory copyright infringement, there is no knowledge of the direct infringement required for vicarious infringement liability.

Each of these elements of vicarious liability have similar sounding equivalents in the DMCA safe harbors. The safe harbor does not apply where the intermediary has the “right and ability to control” the infringing activity and there is a “financial benefit directly attributable” to such activity.<sup>91</sup> As discussed above for contributory liability “knowledge,” the DMCA safe harbors would be of limited utility if the elements of liability were the same as the safe harbor elements—no intermediaries would qualify for vicarious liability protection, and direct liability is not much of a risk.<sup>92</sup> A good example is the ability of intermediaries to remove infringing content. If this amounted to sufficient “control” by the intermediary to be outside the

---

88. *Id.*

89. *Id.* at 249.

90. *A&M Records, Inc.*, 239 F.3d at 1022; *Metro-Goldwyn-Mayer Studios*, 545 U.S. at 930 (“One. . . infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it.”).

91. 17 U.S.C. § 512(c)(1)(B), (d)(2).

92. See Reese, *supra* note 72, at 438–442 (discussing the differences between the parallel requirements for vicarious liability versus a denial of the DMCA safe harbors, and concluding that facts which “could establish a prima facie vicarious liability claim would not suffice to remove the [online service provider] from the safe harbor and allow the claim to proceed” such that the DMCA safe harbor provides some protection from secondary liability). To the extent one disagrees with this position and thinks the DMCA and common law elements are the same, then rather than asking if payment processors should be extended DMCA safe harbors, as this paper does, the question would be whether the DMCA safe harbors should be extended to protect any or all intermediaries from secondary copyright liability.

DMCA protections, the notice and takedown regime of the DMCA would not function because no liability protection would be afforded to intermediaries for the content that is removed.<sup>93</sup> The DMCA removal requirements, thus act as a kind of minimum “floor” to what could be considered the right and ability to control in the statutory context. When the DMCA is not involved, there is no equivalent floor, meaning the right and ability to control may be established more easily.

a. The Right and Ability to Control or Supervise

This element of vicarious copyright infringement requires both proof of legal right to control the infringer and the practical ability to do so. The *Visa* majority found the credit card processors did not meet the threshold for right and ability to control at common law. The plaintiff, Perfect 10, argued the credit card companies had sufficient control by virtue of their merchant rules, imposed on banks and merchants by Visa and MasterCard. These rules require investigation by member banks of suspected illegal conduct by merchants and termination of merchant’s participation in the payment network if certain illegal activity is found. The majority rejected this as establishing the right and ability to control the merchants, drawing a distinction between the ability of credit card companies to “affect” infringement through a refusal to process payments in contrast to the ability to directly control the websites that reproduce, display, and distribute infringing works. It reasoned that the payment processors could not supervise the infringing acts on the websites of their customers and, further, have no ability to remove or block the infringing images. The majority draws an analogy to the *Amazon* case, where Google’s terms and conditions allowed it to terminate AdSense partnerships based on copyright violations.<sup>94</sup> This was found insufficient to provide Google with control over direct infringement of copyright by third-party websites because third-party infringement could continue even if the participation in Google’s ad program was terminated.

As with the arguments on contributory infringement, the analysis contrasts *Fonovisa* and *Napster*, in which the focus was on the provision of facilities and the defendant’s right to remove individual infringers from “the very place the infringement was happening.”<sup>95</sup> The majority also makes a slippery slope argument, arguing software and hardware providers and even utility companies contribute to the viability of a business but should not be held liable for copyright infringement by that business. Like payment processors, their refusal of service could impair the ability of the business to

---

93. *See id.* at 439.

94. *Visa*, 494 F.3d at 803.

95. *Id.* at 798, 805.

operate, but they are not liable because they lack “sufficient control over the actual infringing activity.”<sup>96</sup>

In his strongly worded dissent, Judge Kozinski takes the opposite position on the significance of the terms and conditions. He finds that the payment processors have the requisite authority to stop or limit infringement by virtue of their terms and condition of service, which expressly prohibit illegal activity by merchants. He concludes that control need not constitute an ability to completely stop the infringing conduct because the standard established in *Amazon* requires only the ability to “stop or limit” the infringing conduct.<sup>97</sup> The *Amazon* test also asks whether there is a practical ability to stop infringement, which he finds payment processors have, although there is not an “absolute right to stop” infringement, as the majority requires. The dissenting opinion emphasizes the correlation between risk of liability and control; the risk disappears for more remote third parties—like the utility companies envisaged by the majority—because they “lack the legal right to stop the infringement.”<sup>98</sup> He rejects the majority’s contention that payment systems are somehow less “directly intertwined” with the infringement than software in cases such as *Napster*. As in the contributory copyright infringement analysis, Judge Kozinski’s view is that payment forms an integral, inseparable part of the infringing transaction.<sup>99</sup>

#### b. Financial Benefit

The second element of vicarious liability, a direct financial benefit, is satisfied if the infringing material draws users or increases the attractiveness of the defendant’s service.<sup>100</sup> The benefit need not be directly correlated to the sale of the infringing works.<sup>101</sup> The financial benefit requirement has been easily met in cases where vicarious liability has been imposed, such as *Napster* and *Fonovisa*.<sup>102</sup>

Since there was no right and ability to supervise the infringing conduct found for Visa/MasterCard, the majority in *Visa* declined to rule on the latter question of whether there was a financial benefit for the credit card processors. But Judge Kozinski’s dissent observes at multiple points that the de-

---

96. *Id.* at 806.

97. *Id.* at 819 (Kozinski, J. dissenting).

98. *Id.* at 821 (Kozinski, J., dissenting).

99. *See* discussion *supra* Section I.A.1.

100. *CCBill*, 488 F.3d at 1117 (citing *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004)).

101. *See, e.g., Fonovisa, Inc.*, 76 F.3d at 263 (finding rental of swap meet grounds to offending vendors sufficient to allege direct financial benefit).

102. *See also* *Bartholomew*, *supra* note 39, at 452 (referencing *Arista Records, Inc. v. Flea World, Inc.*, No. 03–2670, 2006 U.S. Dist. LEXIS 14988, at \*41–44 (D.N.J. Mar. 31, 2006) (holding a flea market’s set fees for vendors satisfy this requirement, even though only 9% of customers at the flea market came to purchase CDs and an unknown number of them were seeking infringing copies)).

fendants are profiting from the services they provide to infringing websites,<sup>103</sup> and that suggests that the fees on each payment processed for infringing goods might satisfy the direct financial interest element.

### 3. Applying Secondary Copyright Infringement Analysis to PayPal

Although the *Visa* case provides protection for credit card companies from secondary infringement liability, that protection is far from bulletproof for other online payment processors. The majority's reasoning in *Visa* comes across as results-oriented. Imposing liability on Visa and MasterCard could have brought with it broader chilling effects for online commerce, as well as statutory damages, all of which the majority seemed striving to avoid.<sup>104</sup> But the net result was a dissenting opinion with much stronger reasoning, pointing out strained distinctions and inconsistencies with prior cases in the majority. The strength of the dissent in *Visa* is reinforced by its later adoption in the *Gucci* case, which allowed secondary trademark infringement claims to proceed against payment processors.

The discussion below applies both the majority and the dissent's reasoning in *Visa* to PayPal's business model in an analysis of contributory and vicarious copyright infringement. It is necessarily a general analysis, and specific facts on infringing conduct could change the conclusions. Under the majority's reasoning, none of the theories of secondary liability are likely to be established, although arguments for material contribution are marginally stronger for PayPal than for traditional payment processors. The risk lies in the *Visa* dissent's reasoning, where factual differences in the business of PayPal and similar payment processors leave such companies incrementally more exposed to arguments of material contribution or vicarious copyright infringement liability than major credit card companies. Contributory liability still remains a stretch because PayPal lacks sufficient knowledge of the infringing conduct of its merchants, but claims of vicarious infringement liability are arguable. This is not to say such arguments would be successful in court, but, rather, to point out the difference in risk levels and to illustrate the potential for claims by rights holders. This higher risk is exacerbated by the broader legislative and industry trends seeking to involve payment processors in policing online copyright, as discussed in the following sections of this article.

---

103. *Visa*, 494 F.3d at 816 (2007) (Kozinski, J. dissenting) (stating that the defendants "know about the infringements; they profit from them"); *id.* at 810 (acknowledging Perfect 10s' arguments that the "defendants do not want to lose the substantial revenues and profits they receive from the websites").

104. Bridy, *supra* note 4, at 1538–39.



a. Applying Contributory Copyright Infringement Analysis to PayPal

This Section considers how the analysis of material contribution, inducement, and knowledge might apply to PayPal in assessing claims of contributory copyright infringement.

i. PayPal's Risk of Materially Contributing to Copyright Infringement by Users

PayPal and eBay were part of the same company for thirteen years, until the spinoff of PayPal in 2015. This is significant because together the companies created previously unavailable opportunities for small online sellers and buyers.<sup>105</sup> PayPal gained its initial traction by focusing on small customers, and the company's fortunes rose along with eBay's.<sup>106</sup> PayPal has grown exponentially, and processed a total payment volume of approximately \$354 billion globally in 2016.<sup>107</sup> Although PayPal has since split from eBay, these "micro merchants" continue to drive PayPal's business today.<sup>108</sup> In 2016, PayPal processed an average of only thirty-one payments for each active customer.<sup>109</sup>

PayPal offers two key payment functions: the ability to pay via the PayPal feature itself and the ability to accept credit card payments. For the latter, PayPal itself acts as the merchant of record with Visa and MasterCard on behalf of its customers, rather than each of those merchants having a direct account with Visa or MasterCard. Although oversimplifying some-

---

105. THOMAS EISENMANN AND LAUREN BARLEY, HARVARD BUSINESS SCHOOL CASE STUDY, PAYPAL MERCHANT SERVICES 1 (Mar. 13, 2007) (approximately 78% of the transactions on eBay were processed using PayPal around 2007); see also Vauhini Vara, *Why eBay and PayPal Broke Up*, THE NEW YORKER, Oct. 1, 2014, <http://www.newyorker.com/business/currency/eBay-paypal-broke> (early in PayPal's business lifecycle, eBay also accounted for most of PayPal's transactions, but this has faded to around 30%).

106. See Will Morton, *Check It Out: The Web is suddenly crowded with online-payment services; Here's how they compare*, WALL ST. J., Dec. 10, 2001, at R13 ("The business of online money transfers between individuals grew out of the Internet auction phenomenon, which brought small sellers and buyers onto the Web and created demand for a quick, reliable way to make payments and get the merchandise sent.")

107. PayPal Holdings Inc., Annual Report (Form 10-K), at 41 (Feb. 8, 2017).

108. Letter from PayPal, to J. Johnson, Secretary, Bd. of Governors of the Fed. Reserve Sys., Re: Regulation II, Debit Card Interchange Fees and Routing; Docket No. R-1404 (Feb. 22, 2011) ("PayPal enables a variety of micro merchants to more easily accept payments by providing them with various value-added services, including underwriting the risk of transaction reversals (such as those from consumer disputes) and refunds."); Letter from PayPal to Ms. Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System Re: Proposed rules regarding global remittance services, July 22, 2011, [http://www.federalreserve.gov/secrs/2011/july/20110729/r-1419/r1419\\_072211\\_83811\\_470495842711\\_1.pdf](http://www.federalreserve.gov/secrs/2011/july/20110729/r-1419/r1419_072211_83811_470495842711_1.pdf) (indicating that although PayPal enables peer to peer money transfers, more than 94% of the payments that PayPal processes are for commercial purposes, at least as of 2011. This statistic may change as PayPal increasingly moves into the peer-to-peer payments space, such as through its 2013 acquisition of the payment app Venmo).

109. *Supra* note 107 at 41.

what, PayPal essentially offers the service of allowing merchants to use PayPal's central-merchant account to accept credit card payments for the merchant's business.<sup>110</sup> PayPal therefore enables online payments for sellers who cannot qualify for credit card merchant accounts directly<sup>111</sup> or who do not want to jump through the hoops to obtain their own accounts. PayPal pioneered this "merchant of record" business model for credit card payments, which has since become popular among other online payment services.

PayPal was essential in the proliferation of small online sellers on platforms like eBay because it solved the most intractable barrier to online transactions between strangers—a lack of trust. Traditional payment methods such as cash or checks demand that one party, usually the customer, vest their trust in the other, sending payment in hopes that the goods would arrive, and be of the promised quality. These payment methods offered little or no security for the provided payment information. There was minimal ability to claw-back funds if the products were not delivered or not as advertised. PayPal's intervention was revolutionary because it greatly reduced this trust problem by acting as an escrow agent. PayPal accepts payment from the consumer and then relays that payment to the merchant for a fee. The merchant does not receive the customer's payment details. This enabled transactions to be carried out with confidence, even if the seller and buyer were unknown to each other, because PayPal added both security and control over funds. Even now, PayPal advertises its "Purchase Protection" as a consumer-facing sales feature, which provides the buyer with a refund if the transaction goes awry.<sup>112</sup>

PayPal's appeal to small merchants also stems from its lower cost than credit card payment processing. PayPal charges the same fees regardless of who the customer is or what mode of payment is used. Traditional merchant credit card services vary the fees charged to merchants significantly based on the card used by the customer, and merchants are required to accept all cards regardless of the fee imposed. PayPal offers lower, more consistent fees than credit cards do, and this is a central aspect of PayPal's promotion

---

110. See, e.g., *PayPal Accept Credit Cards Online*, <https://www.paypal.com/webapps/mpp/accept-credit-cards> (last visited Sept. 13, 2016).

111. Katy Jacob et al., *Payments Pricing, Who Bears the Cost?: A Conference Summary*, CHICAGO FED. LETTER number 266a, at 5 (Sept. 1, 2009) ("[P]ayPal also provides smaller merchants that cannot get merchant accounts at banks access to electronic payments systems.").

112. See, e.g., *PayPal Purchase Protection*, <https://www.paypal.com/us/webapps/mpp/paypal-safety-and-security> (last visited Sept. 13, 2016) ("[W]e protect you from checkout to delivery and use the latest anti-fraud technology to help spot problems before they happen. We never reveal your financial info to sellers. And if something goes wrong with an order, we'll investigate. If your transaction qualifies for Purchase Protection, we'll reimburse you for the full purchase price plus any original shipping costs.").

to small merchants.<sup>113</sup> As a result, PayPal's business is driven by many small customers seeking this value, more so than Visa's or MasterCard's.

Although smaller merchants are not necessarily infringing merchants, PayPal's partner, eBay, has known infringement problems amongst its merchants. For example, in a prominent case involving the sale of Tiffany jewelry on eBay, more counterfeit jewelry than authentic jewelry was found on the website.<sup>114</sup> Since PayPal and eBay services are historically intertwined, similar infringing conduct among PayPal's merchants could easily exist. Although far from conclusive, an initial case search also turned up multiple anecdotal examples of copyright infringement claims against small merchants using PayPal accounts for their allegedly infringing transactions.<sup>115</sup> The instances of infringing conduct among PayPal customers more broadly, particularly in comparison to more traditional payment methods, would be an interesting area of further study. It may also be that infringing merchants are more likely to be smaller merchants because building a successful, large scale business based on infringement is difficult in the face of active copyright enforcement.

PayPal's integral role in the viability of many of its small merchant's businesses provides a stronger argument that PayPal supplies the "facilities" for the infringement, at least relative to the role of major credit card companies. The majority in *Visa* concluded that because "other viable funding mechanisms are available," infringement could continue on a wide scale even if Visa and MasterCard were not involved (and therefore the card companies had not materially contributed). This seems less accurate for many of PayPal's merchants. Although there are more alternative online payment options now than at the time of the *Visa* case, PayPal remains by far the most popular, trusted, and established. At least compared to merchants who are qualified to obtain Visa or MasterCard accounts, like those in the *Visa* case, it seems likely that PayPal's merchants have fewer viable funding mechanisms. Based on the *Visa* majority, that makes arguments that PayPal is supplying a form of "facilities" to its merchants more likely.

PayPal would likely be found to be a material contributor to infringement under Judge Kozinski's dissent. This reasoning rejects the analysis of

---

113. See, e.g., *Why PayPal?*, <https://www.paypal.com/us/webapps/mpp/brc/why-paypal> (last visited Sept. 13, 2016) (promoting lower PayPal fees (2.9% of the total transaction, plus \$0.30 per transaction) compared to traditional merchant card services fees. PayPal also claims it reduces payment processing costs because there are fewer chargebacks, less fraud, and fewer customer complaints than with traditional credit card processing services.).

114. *Tiffany (NJ) Inc.*, 600 F.3d at 97–98 (referencing a study by Tiffany that found 75.5% of test purchases on eBay were counterfeit jewelry. Although the court questioned the methodology of this finding, it agreed that a "significant portion of the 'Tiffany' sterling silver jewelry listed on the eBay website . . . was counterfeit").

115. See, e.g., *Pearson Educ., Inc. v. Ishayev*, 9 F. Supp. 3d 328 (S.D.N.Y. 2014); *Tory Burch Ltd. Liab. Co. v. Doe*, No. 12 C 7163, 2012 U.S. Dist. LEXIS 142554 (N.D. Ill. Oct. 2, 2012).

the number of alternative means to infringe as irrelevant in determining materiality of the contribution to infringement, which can always be carried out some other way. Instead the question is whether PayPal “substantially assists” in the infringement. The dissent views involvement in payment for infringing works as direct involvement in the infringement. On this reasoning, PayPal’s enabling payment for infringing goods would be a material contribution. And there is an argument that PayPal provides more substantial assistance to its merchants’ infringing transactions than Visa or MasterCard, for the same reasons explained above; PayPal is not merely tangential to enabling the businesses of its small merchants, as they might not be merchants at all but for the pioneering PayPal business model. If the *Visa* dissent’s approach signals the direction of future law, as the adoption in *Gucci* might suggest, then online payment processors face an increasing risk of contributory copyright liability.

#### ii. PayPal’s Potential Knowledge of Direct Infringement

As with other payment processors, PayPal likely has general knowledge of the type of transactions it is processing, some knowledge of the nature of its vendors’ businesses, and some more specific knowledge of transactions charged back through PayPal’s purchase-protection services. Although information on the type of transaction reflects a certain level of factual “knowledge,” it falls short of the high level of specificity that has been required for liability in past contributory copyright infringement cases. Most cases have held that a general knowledge that one’s service could be used to infringe copyright, or even that it is generally being used to do so, is not sufficient for contributory liability.

However, if the more relaxed *Gucci* approach to “knowledge” was applied in copyright law, PayPal could well be found to have knowledge of direct infringement. The *Gucci* case found plausible knowledge based on routine actions like merchant vetting before account opening and customer complaints resulting in chargebacks. As in *Gucci*, whether PayPal had sufficient knowledge would depend on the facts, such as how closely PayPal looks at its merchant’s businesses before providing them with services.

*Gucci* illustrates the factual differences in the roles of various payment intermediaries that influence their level of knowledge. Although this paper often discusses payment processors generally, their roles vary widely. Visa and MasterCard generally do not have direct merchant contact; they interact with banks in an authorization, clearing, and settlement role.<sup>116</sup> In contrast, acquirers—meaning the banks and other parties who bring merchants into card networks (as in *Gucci*)—vet merchants and see chargebacks. The po-

---

116. For a helpful and detailed discussion of the distinctions between the parties involved in payment processing, see Kelly K. Yang, *Paying for Infringement: Implicating Credit Card Networks in Secondary Trademark Liability*, 26 BERKELEY TECH L.J. 687 (2011).

tential implications of this distinction are emerging in the cases canvassed above; Visa and MasterCard, who have more remote relationships with merchants, were not liable for secondary infringement in *Visa*, whereas a plausible case was made out in *Gucci* against the payment intermediaries who interacted more closely with the merchants.

Online payment processors like PayPal fall somewhere in between. The application for PayPal merchant services requires the business to be described by type and category, but it is not clear what additional vetting of merchants occurs after that stage. If cases like *Gucci* signal increasing likelihood of knowledge being found for online payment processors, then the higher bar for knowledge under a DMCA-like system looks preferable for payment processors. It would reduce their risk of being found to have knowledge sufficient for secondary liability through routine conduct like that in *Gucci*.

### iii. Applying the Inducement to Infringe Analysis to PayPal

The inducement branch of contributory copyright infringement seems unlikely to be a strong argument against PayPal's business. The cumulative result of the inducement cases is a somewhat blurry scale, from software systems promoted for the purpose of piracy in *Grokster*, to the facilitation of high-risk payment accounts in *Gucci*, to the marketing of credit cards as a means of paying for goods online in *Visa* which did not constitute inducement. On this scale, it would be hard to argue that PayPal's system was designed for the explicit purpose of facilitating infringement, as the court found for *Grokster*. And, while *Grokster*'s inducement was based in part on its failure to create tools to filter infringing content, PayPal has actively developed filtering and control tools and, in some cases, has chosen to block categories of transactions in an effort to reduce infringement.<sup>117</sup>

*Grokster*'s liability was also based on its efforts to target customers known to be infringers because they used a prior infringing service, Napster. Not all Napster users were infringing, but many were known to be. A version of this argument could be applied to PayPal, whose bread and butter is smaller, online customers who may not be able to obtain a Visa or MasterCard account. PayPal certainly targets small, online merchants in its advertising. Not all PayPal users are infringing, but existing cases and the history with eBay suggests some proportion are, so PayPal's advertisements to small users could be seen as targeting infringing users. Although such arguments might be made, they stretch the logic in *Grokster* too far. PayPal's customer base is not a known group of predominantly infringing users like *Grokster*'s

---

117. See, e.g., Pincen Masons, *PayPal Terms Require File-Sharing Operators to Let It Monitor for Pirate Content*, OUT-LAW.COM, <http://www.out-law.com/en/articles/2012/july/paypal-terms-require-file-sharing-operators-to-let-it-monitor-for-pirate-content/> (July 12, 2012); See also the discussion on PayPal's block with respect to VPN services, below.

was—they are a largely uncharacterized group with a likely larger proportion of legitimate users. PayPal can distinguish the *Grokster* case by arguing it is advertising merely to small customers, not infringing customers, and equating between the two is an unsubstantiated generalization.

As with *Visa's* reasoning applied to Visa and MasterCard's general promotion of their payment services, it is more likely that PayPal's general promotion to small merchants does not amount to inducing infringement. Inducement would require more specific instances of advertising by PayPal for the use of its products in infringement. PayPal has certainly stopped short of marketing specifically to “replica” companies like Durango did in the *Gucci* case. A finding of inducement to infringe for PayPal based on the reasoning in *Visa* therefore seems unlikely.

#### b. Applying Vicarious Copyright Infringement Analysis to PayPal

PayPal likely meets the element of direct financial benefit required to find vicarious infringement of copyright through its merchants. When infringing goods are purchased by end consumers from its merchants, PayPal earns a fee directly from the merchant on that transaction. The more difficult question is whether PayPal meets the second element of vicarious copyright infringement, which would require PayPal to have the right and ability to control its merchant's infringement of copyright.

Under the majority's reasoning in *Visa* on the right and ability to control, PayPal is unlikely to face vicarious copyright infringement liability because, like the credit card defendants, it lacks sufficient control over merchant conduct. PayPal cannot remove websites from the Internet or block the distribution of their content. PayPal may, as discussed in the contributory copyright infringement analysis above, have a greater ability to exert financial pressure on its merchants than credit card companies, based on the assumption that more PayPal merchants lack alternative payment methods. But *Visa* dictates that PayPal's ability to affect merchant payments in such a manner is insufficient to constitute direct control over the acts of reproduction, alteration, and distribution of copyrighted content by such merchants. The “control and supervise” element of vicarious liability would not be met.

However, PayPal would face a greater risk of vicarious liability for copyright infringement than major credit card companies under the reasoning in Judge Kozinski's dissent. First, at the outset of his evaluation of whether there is “control,” Judge Kozinski observes that blocking the ability to accept credit cards would be a “heavy blow” to the websites because of the escrow agent role that credit cards play in ensuring customers can reverse the transaction if the goods are not satisfactory. This argument has even greater force for PayPal, whose escrow function is central to its value proposition. PayPal's popularity in online transactions stems from the trust it created as an escrow agent for online auction payments when a lack of rela-

tionship or payment recourse between buyers and sellers would otherwise have precluded the transaction. PayPal's escrow agent role is central to facilitating the business of its customers, even more so than the credit cards at issue in *Visa*.

Second, Judge Kozinski found that the Visa and MasterCard terms of service gave them authority to control infringing sales by merchants.<sup>118</sup> The rules permitted the credit card companies to require member merchants to cease illegal activity—such as copyright infringement—as a condition of continuing right to receive credit card payments from the defendants.<sup>119</sup> Cutting off the payment services in such a manner would stop or limit the direct infringement. Similarly, PayPal's User Agreement expressly grants PayPal the right, in its sole discretion, to terminate account access if a user engages in "restricted activities." Such activities include violation of any law and, more specifically, "sell[ing] counterfeit goods."<sup>120</sup> Even though PayPal does not have physical control over the infringing goods sold, the company has the direct ability to terminate infringer's accounts, which satisfies the control element under the reasoning of Judge Kozinski's dissent.

Judge Kozinski's approach could backfire in the absence of an infringement safe harbor for online payment processors. If payment processors face liability for merchant actions because their terms of use prohibit infringing conduct, the simplest solution, in theory, is to delete the contractual clause providing that control. This would be an extreme measure in practice, but not every intermediary is necessarily a good corporate citizen. Under Judge Kozinski's analysis, such deletion would relieve the payment processor of vicarious liability risk because the company would no longer have the direct legal ability to control the infringing conduct of its users. Judge Kozinski does not address this theoretical impact in his dissent. The DMCA safe harbors offer a means of guarding against this scenario by encouraging good-faith take-down by intermediaries without imposing liability for secondary infringement.

### B. Legislative Leanings Toward Payment Processor Enforcement Online

By 2011, policy recommendations and proposed legislation had begun pushing toward a greater role for payment processors in fighting online infringement. The Registrar of Copyrights, an American Bar Association (ABA) report, and the failed *Stop Online Piracy Act* (SOPA) and its Senate counterpart the *Protect IP Act* (PIPA) have all proposed increased obliga-

---

118. *Id.*, at 817.

119. *Id.*, at 816.

120. *PayPal User Agreement*, (effective as of July 27, 2017), <https://www.paypal.com/webapps/mpp/ua/useragreement-full#9> (restricting the sale of counterfeit goods and permitting the termination if restricted activities are engaged in).

tions on payment processors to deny services to merchants with copyright infringing websites.

The Registrar of Copyrights, the director of the U.S. Copyright Office, lamented the proliferation of “rogue” foreign websites violating IP rights beyond the reach of the U.S.<sup>121</sup> In the same statement before the House Committee on the Judiciary, she advocated for a “follow the money” approach that cuts off U.S. payment mechanisms and advertising of infringing foreign sites.<sup>122</sup> The Registrar argued that cutting off payment methods was an efficient and effective means of depriving such websites of customers, particularly because consumers are suspicious of websites that do not accept standard payment types.<sup>123</sup>

Similarly, the ABA’s Intellectual Property Section issued a report in 2014 that encouraged Congress to enact more effective laws to deter online piracy and counterfeiting by foreign websites.<sup>124</sup> The ABA called for legislation enabling orders to be made against financial service providers to freeze customer funds obtained by “counterfeiting” websites.<sup>125</sup> Financial-service providers have responded to calls for such legislation by requesting safe harbors to protect against wrongful interference claims by the targeted websites.<sup>126</sup>

The ABA argues payment processors are well-positioned intermediaries to freeze funds because of their existing fraud-detection systems.<sup>127</sup> The report references four recent cases where asset-freezing orders have been issued against payment processors by U.S. District Courts.<sup>128</sup> Interestingly, at least two of these cases involved orders to freeze PayPal accounts, but none

---

121. *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Parts I & II: Hearing on H.R.112-153 Before the H. Comm. on the Judiciary, Subcommittee on Intellectual Property, Competition, and the Internet*, 112th Cong. 1, 18 (2011) (written statement of Maria A. Pallante, Acting Register of Copyrights), [https://judiciary.house.gov/\\_files/hearings/printers/112th/112-153\\_65186.pdf](https://judiciary.house.gov/_files/hearings/printers/112th/112-153_65186.pdf).

122. *Id.* at 19–25; 108 (suggesting that legislation be enacted allowing customs enforcement agencies to request a court order that requires payment processors, including “credit card companies and payment intermediaries such as PayPal,” to stop providing services for rogue website to consumers in the U.S.).

123. *Id.* at 24.

124. AMERICAN BAR ASSOCIATION SECTION OF INTELLECTUAL PROPERTY LAW, *A Section White Paper: A Call for Action for Online Piracy and Counterfeiting Legislation* (2014), at ix [http://www.americanbar.org/content/dam/aba/administrative/intellectual\\_property\\_law/advocacy/ABASectionWhitePaperACallForActionCompositetosize.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/administrative/intellectual_property_law/advocacy/ABASectionWhitePaperACallForActionCompositetosize.authcheckdam.pdf).

125. *Id.* at 27–28.

126. *Id.* at 28.

127. *Id.*

128. *Id.* at 27 (referring to *True Religion v. Xiaokang Lei*, No. 11-cv-8242 (HB), at 10 (S.D.N.Y. 2011) (temporary restraining order); *Philip Morris USA, Inc. v. Jiang*, No. 11-cv-24049, 2011 U.S. Dist. LEXIS 142630, at \*9 (S.D. Fla. 2011) (preliminary injunction); *Deckers Outdoor Corp v. Doe*, No. 11 C 10, 2011 U.S. Dist. LEXIS 119448, at \*15–\*19 (ND. Ill. 2011) (default judgment); and *Hermès Int’l et al. v. John Doe et al.*, No. 12 Civ. 1623, at 6–7 (S.D.N.Y. 2012) (default judgment and permanent injunction)).



of the orders were against traditional credit card processors.<sup>129</sup> One possible explanation for PayPal being a more popular target for such orders is that PayPal users can maintain a balance with the company. That balance can be targeted by freezing orders while transaction-by-transaction payment processing cannot. Another possible explanation is that PayPal's merchants are more likely to offer infringing goods that make such orders necessary.

The contentious *Stop Online Piracy Act*, and its Senate counterpart the *Protect IP Act*, also proposed that payment processors be required to cease providing services to blacklisted infringing websites.<sup>130</sup> The pair of bills were proposed by a coalition of intellectual property rights advocates, including the strong motion picture and sound recording lobbies.<sup>131</sup> The headline news was the intense opposition to the bills by advocates of freedom of expression and the open Internet, who were concerned about over-broad remedies that would allow for the removal of large amounts of non-infringing online content.<sup>132</sup> The unprecedented opposition meant these bills were abandoned before they were brought forward for the necessary votes.<sup>133</sup> The headline-capturing, big-picture issues also meant the payment processor provisions in the same bills remained largely under the radar.

SOPA proposed a new notice and blocking regime targeted at “black-listed” domains involved in intellectual property infringement, provocatively labeled as Internet sites “dedicated to theft of U.S. property.”<sup>134</sup> Advertising networks and payment processors, upon notice, would be required to take “technically feasible and reasonable measures” to cut off payment processing for such sites for any transaction involving customers located in the U.S.<sup>135</sup> Like DMCA notices, the SOPA/PIPA notices include a statement that the holder of the intellectual property right has a good faith belief that the use is not authorized, including by law.<sup>136</sup> The bills also contemplated a

---

129. *Hermès Int'l et al. v. John Doe et al.*, No. 12 Civ. 1623 (S.D.N.Y. 2012); *True Religion v. Xiaokang Lei*, No. 11 Civ. 8242 (S.D.N.Y. 2011).

130. *Stop Online Piracy Act (SOPA)*, H.R. 3261, 112th Cong. (1st Sess. 2011); *Protect Intellectual Property Act (PIPA)*, S. 968, 112th Cong. (2011). The predecessor bill to PIPA was the *Combating Online Infringement and Counterfeits Act (COICA)*, S. 3804, 111th Cong. (2010).

131. Bridy, *supra* note 4 at 1540.

132. See, e.g., *SOPA/PIPA: Internet Blacklist Legislation*, ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/issues/coica-internet-censorship-and-copyright-bill> (last visited October 14, 2017); see also, Bridy, *supra* note 4, at 1540–41. (recounting the dramatic responses to Wikipedia and other significant websites going “dark” for one day in protest, prompting unprecedented numbers of people to contact their Congressional and Senate representative to express opposition to the bills).

133. Andrew P. Bridges, *SOPA Didn't Die. It Just Became Soft SOPA.*, *Intellectual Property Bulletin Summer 2013*, FENWICK & WEST LLP (Sept. 25, 2013), <http://www.fenwick.com/Publications/Pages/Intellectual-Property-Bulletin-Summer-2013.aspx#Sopa>.

134. *Stop Online Piracy Act* § 103.

135. *Id.* at § 103(b)(1). The provisions related to payment processors were fairly similar in SOPA and PIPA. See Bridy, *supra* note 4, at 1542.

136. *Stop Online Piracy Act* § 103(b)(4)(A).

counter-notice regime under which the targeted domain holder could dispute the initial notice. Upon receipt of such a counter-notice, the payment processor need not take further action until the complaining party obtains and serves the processor with a court order against the domain.<sup>137</sup> Once the court order is served, the payment processor is again obligated to cut off services to the website or else they *themselves* can be made the subject of an order to comply.<sup>138</sup> A knowing and willful failure to comply with the order against the payment processor can result in monetary damages. Payment processors who comply with notices or orders are protected from litigation arising from actions to reasonably comply with the proposed legislation and from actions by users to circumvent access restrictions on foreign sites.<sup>139</sup>

The proposed SOPA regime placed payment processors front and center in battling online infringement. It weighed the balance heavily in favor of blocking payment because, unlike the opt-in DMCA scheme, it provides for orders and even monetary damages against payment processors who refuse to block services. Interestingly, payment processors were split on their support or opposition to SOPA; Visa and MasterCard ultimately expressed support,<sup>140</sup> while PayPal opposed the bills.

The opposition to SOPA and PIPA's other provisions was rooted in concern over blocking of non-infringing content hosted on the same servers as infringing content, potentially violating freedom of expression rights. The same criticism of over-broadness can be levied at the payment processor provisions. The liability protection for processors is contingent on entirely blocking payments to websites that are blacklisted. Yet the legislation implies the blocks can apply to much more than websites that *directly* infringe by using waffle words like "engages in, enables, or facilitates" infringement and "other affirmative steps taken to foster infringement."<sup>141</sup> This casts a net broad enough to catch sites with a mixture of legal and illegal content. One notice of one instance of infringement could mean the loss of all payment services, preventing transactions for non-infringing content, and even blocking payments for non-infringing but "facilitating" websites.

---

137. See Pallante, *supra* note 121.

138. Stop Online Piracy Act §§ 103(d)(2)(A)(i), 103(d)(4)(B).

139. Id. § 103(d)(5).

140. See *Stop Online Piracy Act: Hearing on H.R. 3261 Before the H. Comm. on the Judiciary*, 112th Cong. 82–83, 91 (2011) (statement of Linda Kirkpatrick, Group Head, Customer Performance Integrity, Mastercard Worldwide); *List of Supporters and Opponents of H.R. 3261*, OPENCONGRESS, [https://www.opencongress.org/bill/hr3261-112/bill\\_positions](https://www.opencongress.org/bill/hr3261-112/bill_positions) [[https://web.archive.org/web/20160228085636/https://www.opencongress.org/bill/hr3261-112/bill\\_positions](https://web.archive.org/web/20160228085636/https://www.opencongress.org/bill/hr3261-112/bill_positions)] (listing PayPal in opposition and Visa in support).

141. Stop Online Piracy Act § 103(a)(1) (defining the phrase "Internet site is dedicated to theft of U.S. property").

### C. Payment Processors “Voluntarily” Police Copyright Infringement

This Section considers the implications of the recent agreement among payment processors to centrally and voluntarily block payment processing for allegedly infringing merchants, and the unilateral blocking of services by payment processors and other intermediaries.

#### 1. The Payment Processor Agreement: Few Merchant Rights, Weak Payment Processor Liability Protections

Although SOPA and PIPA died as bills, their shadow hung heavy over payment processors. The threat of SOPA/PIPA-like legislation is credited with driving an industry-wide “voluntary” best practices agreement among payment processors to facilitate denials of service for copyright infringing websites.<sup>142</sup> In June 2011, an agreement on best practices was reached between all of the major payment processors: American Express, Discover, MasterCard, PayPal, Visa, and approximately thirty-one rights holders (the “Payment Processor Agreement”).<sup>143</sup> The parties agreed to abide by best practices to “stop sites distributing counterfeit and pirated goods from conducting financial transactions through payment processors.”<sup>144</sup>

Whether the Payment Processor Agreement was truly “voluntary” has been called into question, with one author labeling it “non-regulatory regulation.”<sup>145</sup> Although the agreement is technically voluntary, all major payment processors agreed to it under threat of SOPA/PIPA. In the words of one Congressman, SOPA/PIPA focused a spotlight on intermediaries and “helped motivate an important shift in the willingness of some parties to engage more aggressively in negotiating to develop some of the best practices” in online copyright infringement.<sup>146</sup> It was “highly encouraged and

---

142. Bridy, *supra* note 4, at 1543 (describing how the online intermediaries that would have been subject to SOPA/PIPA instead implemented voluntary blocking agreements, under the pressure of the IPEC).

143. U.S. INTELLECTUAL PROP. ENF’T COORDINATOR, 2011 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT 46 (2012), [https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/IPEC/ipec\\_annual\\_2011\\_report-new.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/IPEC/ipec_annual_2011_report-new.pdf) [hereinafter IPEC 2011 ANNUAL REPORT] (indicating an agreement had been reached between the above-mentioned parties in June 2011); INTERNATIONAL ANTI-COUNTERFEITING COALITION, BEST PRACTICES TO ADDRESS COPYRIGHT INFRINGEMENT AND THE SALE OF COUNTERFEIT PRODUCTS ON THE INTERNET, (on file with the author, courtesy of Professor Annemarie Bridy) (“Payment Processor Agreement”). The June 2011 agreement does not appear to be publicly available.

144. IPEC 2011 ANNUAL REPORT, *supra* note 143, at 46. Other payment processors such as MoneyGram, PULSE and Western Union have since signed on to the agreement.

145. Bridy, *supra* note 4 at 1543.

146. *Role of Voluntary Agreements in the U.S. Intellectual Property System: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 2 (2013) (statement of Rep. Mel Watt, Member, H. Comm. on the Judiciary), <https://judiciary.house.gov/wp-content/uploads/2016/02/113-49-82846.pdf>. See House Judiciary Committee hearings on copyright reform, *supra* note 10 (raising the question

supported” by the Intellectual Property Enforcement Coordinator (IPEC), an office of the White House established in 2009 that convenes and participates in the negotiations of such agreements.<sup>147</sup> The Administration, through IPEC, has long taken the position that payment processors and other intermediaries should voluntarily engage in steps to support copyright holders.<sup>148</sup> If the industry chooses not to collaborate with IPEC, the agency can make recommendations on further legislative measures,<sup>149</sup> leaving little choice for industry participants but to improve their policing of infringement online.

The Payment Processor Agreement sets out high-level best practices for payment processors to address copyright infringement and counterfeit product sales online.<sup>150</sup> The Agreement provides for rights holders to file complaints about infringing sites in order to have payment processing blocked. The complaint must include a description of the infringement, including the website and evidence proving the allegation, evidence of ownership of the intellectual property in question, and evidence that the payment processor’s services could theoretically be used to buy the infringing product.<sup>151</sup> Similar to the DMCA notice regime, the notice contains an attestation from the rights owner that, to the best of their knowledge, the use of the intellectual property by the website is not authorized by license or the law.<sup>152</sup> Each payment processor can determine the specifics of their own process within these general best practices.

Payment processors and the governmental International AntiCounterfeiting Coalition (IACC) started a central, online portal called “Rogue Block” to facilitate rights holders’ complaints to payment processors in conjunction with the Payment Processor Agreement.<sup>153</sup> Since its com-

---

again as to whether Congress should create incentives for voluntary systems to address infringement).

147. IACC, *Rogue Block*, IACC.ORG, <http://www.iacc.org/online-initiatives/rogueblock> (last visited September 19, 2016). By 2013, IPEC had “facilitated” several agreements including the payment processor agreement, a Memorandum of Understanding between broadband providers and rights owners and pledges from advertiser networks for online best practices.

148. Bridy, *supra* note 4 at 1543–44 (tracing the increasingly specific statements about IPEC encouraging payment processor voluntary participation in site-blocking).

149. *Id.* at 1545.

150. The terms are imposed, where relevant, on merchant acquirers as well, through their terms of service with the participating payment processors.

151. Payment Processor Agreement, *supra* note 144, sec. 3; KRISTINA MONTANARO, INT’L ANTICOUNTERFEITING COALITION, EXECUTIVE SUMMARY OCTOBER 2012: IACC PAYMENT PROCESSOR PORTAL PROGRAM – FIRST YEAR REVIEW (2013) (describing the Payment Processor Agreement/Rogue Block operation and including an example notice). The IACC role in the scheme is to review the complaints for completeness, then sends them on to the relevant payment processor(s).

152. Payment Processor Agreement, *supra* note 143, sec. 3(c); IACC Executive Summary (2013), *supra* note 151 at 5. Alternatively, the rights holder can provide a DMCA notice or a cease and desist letter.

153. See generally Int’l AntiCounterfeiting Coalition Rogue Block, *supra* note 147.

mencement in early 2012, Rogue Block has resulted in the termination of over 5,000 merchant accounts, impacting over 200,000 websites.<sup>154</sup> This number would likely be higher but for the program's limit of twenty-five complaints per rights holder per month.<sup>155</sup>

The Payment Processor Agreement has some major flaws from the perspective of merchants, including procedural and substantive issues that heighten the risk of over-blocking legitimate commerce. Procedurally, after a complaint is filed, it is not clear exactly what notice is required to be given to the subject merchant. However, the Payment Processor Agreement indicates that the merchant may contest the claim by providing written evidence that it has the right to sell the allegedly infringing product.<sup>156</sup> Statistics suggest these "counter" notices are rare; none were received in the first year of operation,<sup>157</sup> and by the second year, only four had been received, amounting to a response rate of 0.05% of all notices issued.<sup>158</sup> This could be interpreted multiple ways. Perhaps merchants are not disputing complaints because they are not aware of their option to do so, or because of a sense that the power of rights holders and payment processors make such efforts futile. Alternatively, these statistics could indicate that most Rogue Block requests are justified, because the target merchant cannot provide counter-notice evidence of their non-infringement.

Substantively, the blocking decision also seems potentially unfair to merchants. The determinative factor in the payment block is the investigation by the payment processor and whether in its reasonable opinion the merchant is violating intellectual property rights. There is no indication of the extent or nature of the investigation required of the payment processor. Nor is there a statement on the factors that might be determinative in drawing the infringement conclusion. If the payment processor is of the opinion that there is a violation, an initial demand is made to the merchant to cease selling infringing products.<sup>159</sup> If the merchant persists after the warning, the payment processing services must be suspended or terminated for U.S. buyers.<sup>160</sup> The voluntary agreement is light on details for remedial action by merchants who are wrongly sanctioned, and any appeal by the merchant of the decision is to the same payment processor.<sup>161</sup>

---

154. *See Id.*

155. The limit was intended to reduce the burden on the IACC, which acts as an intermediary for the program's notices.

156. Payment Processor Agreement, *supra* note 143 at sec. 6.

157. IACC Executive Summary (2013), *supra* note 151 at 12.

158. IACC 2013 Highlights Report at 2, (indicating 4 of 8,000 notices were challenged) (on file with author, previously available at [http://www.gacg.org/Content/Upload/MemberNewsDocs/IACC\\_2013\\_YearInReview.pdf](http://www.gacg.org/Content/Upload/MemberNewsDocs/IACC_2013_YearInReview.pdf)).

159. Payment Processor Agreement, *supra* note 14 at sec. 7 (warning).

160. *Id.* at sec. 8 (indicating payment "shall" be suspended or terminated, non-voluntary).

161. Bridy, *supra* note 4 at 1561.

Even worse, if the payment processor does *not* think the website is infringing, the agreement contemplates that payment services could still be blocked.<sup>162</sup> If the payment processor finds that the merchant provided credible evidence of non-infringement, the payment processor can then request indemnity from the rights holder and proceed with the block anyway.<sup>163</sup> This gives rights holders significant control over the incentives for blocking and tilts the system in favor of payment processors refusing services to merchants. A denial of payment services to the merchant prevents the sale of all of their products. The result is potential over-blocking, where service is denied to a merchant with a site that contains both infringing and non-infringing content or even predominantly non-infringing content. In fact, the Payment Processor Agreement contemplates on its face that websites could contain both infringing and non-infringing goods for sale.<sup>164</sup>

The operation of the Rogue Block system creates the potential for over-blocking in two further ways. First, the rights holder complaint requires the inclusion of merely “a representative” infringing product.<sup>165</sup> The payment processor does not appear to receive information about the proportion of legal or illegal transactions processed by the merchant that is the subject of a blocking request. Second, the Rogue Block system distributes notices requesting a denial of payment services to all relevant payment processors.<sup>166</sup> This would be roughly equivalent to a centralized DMCA system where notice is given once by the rights holder, but channeled out to prompt action by all ISPs and other online service providers, instead of requiring separate notice to each of these intermediary as the DMCA currently does. Since all major payment processors participate in the system, the centralization makes it more likely the merchant site will be completely shut down, as all of its payment alternatives are blocked. These factors in the voluntary system make over-blocking likely and weigh the system in favor of rights holders.

In contrast to the Payment Processor Agreement, the DMCA regime has at least two features that are beneficial for merchants. First, at least in theory, it channels two-sided disputes into the hands of the judiciary. A DMCA counter notice results in “put back” of the content that was removed, unless and until the complaining rights holder brings legal action to prevent what it sees as infringing activity.<sup>167</sup> This triggers judicial oversight where there is a counter notice, which increases the likelihood that merchant/user rights are taken into account. The benefit of such oversight is evident in recent cases

---

162. Payment Processor Agreement, *supra* note 14 at sec. 11; Bridy, *supra* note 4 at 1561.

163. Payment Processor Agreement, *supra* note 14 at sec. 11.

164. *Id.* at sec. 3(a) (“[i]f only certain items on a website are alleged to be Illegitimate Products. . .”).

165. IACC Executive Summary, *supra* note 151, at 5.

166. *Id.* at 6.

167. 17 U.S.C. § 512 (g)(2)(C).

that have recognized user rights in the DMCA context, such as the requirement that copyright holders consider whether the fair use doctrine permits the use of material the copyright holder otherwise would seek to remove through a takedown notice.<sup>168</sup> Second, on the rare occasions when a merchant challenges a block under the Payment Processor Agreement, there is no indication that their services are restored while the dispute is pending in a manner akin to the DMCA's "put back." Since a payment block could stop the merchant's business from functioning entirely, restoration of services while determining whether the merchant is infringing is significant. Although the DMCA faces criticism about over-takedown and a failure to protect user rights, it still seems like an improvement over the system of the Payment Processor Agreement.

The Payment Processor Agreement seems to have downsides for payment processors as well. There remains some discretion for companies participating in the Payment Processor Agreement since it is framed only as "best practices," and ultimately each payment processor can design their own investigation and response systems.<sup>169</sup> However, under those best practices, the denial of payment services is termed as *mandatory* rather than voluntary if the merchant persists in allegedly infringing sales after an initial warning.<sup>170</sup> This is a major difference from the DMCA, where the intermediary may choose not to respond to a takedown notice and take the chance that it may or may not face secondary liability claims. In contrast, the DMCA regime does not impose an affirmative duty on the intermediary to block infringing content.

The Payment Processor Agreement seems to leave payment processors in an awkward position in which they assume enforcement costs and responsibilities without robust protection from liability. Payment processors are incurring the costs and burdens of a notice and blocking regime in a manner that looks similar to the DMCA system, yet are stuck in a liability sandwich between rights holders and merchants. If rights holders are unsatisfied by the payment processors response to a block request, there is no guarantee of liability protection unless the rights holders waive their right to sue by agreement. Such contractual protection seems contingent on the rights holder being happy about the takedown decisions, making it much more fragile than legislated liability protection offered by the DMCA. If anything, this lack of liability protection could lean payment processors even further toward

---

168. *Lenz v. Universal Music Corp.*, 801 F.3d 1126, 1133 (9th Cir. 2015) (holding that 17 U.S.C. § 512(c)(3)(A)(v) requires copyright holders to consider whether the potentially infringing material is a fair use of a copyright under 17 U.S.C. § 107 before issuing a takedown notification, and that "anyone who . . . makes a fair use of the work is not an infringer of the copyright with respect to such use").

169. Payment Processor Agreement, *supra* note 143, at sec. 1.

170. *Id.* at sec. 8 (indicating payment services "shall" be suspended or terminated if the merchant persists in selling infringing products after the initial warning).

blocking payment in response to notifications, amplifying the impact on merchant rights. When the payment processor chooses to block payment services without an indemnity from the rights holder, it also becomes exposed to potential merchant claims for breach of service terms, as discussed below in the Allofmp3.com case. The current “voluntary” systems appear to be a stick with little carrot for payment processors; the main incentive for participation was trying to avoid a more onerous legislative regime in the vein of SOPA/PIPA.

## 2. Unilateral Denials of Service by Payment Processors

Online payment processors are also engaging in another form of industry self-regulation: unilateral blocks of payment services pursuant to their company terms of service or policies. PayPal accepts reports of alleged infringement on particular websites or webpages through an e-mail and fax system. The report must describe what the rights are, how the website infringes and why the reporting party believes PayPal services are being used to make payment for infringing goods or services.<sup>171</sup> Unilateral denials of payment services present problems both for payment processors when the merchants fight back and for merchants, because the blocking can be extremely overbroad. A payment block is a blunt instrument because it is often all or nothing for a merchant, even if some legal conduct is affected. PayPal’s unilateral system for payment blockades recognizes this risk of over blocking in its infringement reporting form:

I understand that this Report may lead to the temporary or permanent restriction of the PayPal account and/or PayPal services associated with the Webpage. PayPal account restriction has serious consequences, including the inability of the account holder to use PayPal services in connection with any business or transaction, not only those associated with the identified [w]ebpage.<sup>172</sup>

The AllofMP3.com dispute provides the perfect example of both over-blocking of legal merchant activity and the difficult legal position faced by payment processors who unilaterally deny services. The Russian website, AllofMP3.com, enabled downloading of copyrighted songs for a small fee. The service was illegal under U.S. copyright law but legal under Russian copyright law at the time. While a secondary copyright infringement claim was pending in U.S. courts, the International Federation for the Phonographic Industry convinced Visa and MasterCard to voluntarily cease processing all payments for AllofMP3.com. This resulted in blocking of transactions that were legal in Russia. The operator of AllofMP3.com then

---

171. See Infringement Report, PayPal Inc. (last visited Mar. 16, 2016), [https://www.paypalobjects.com/webstatic/ua/pdf/US/en\\_US/infringementreport.pdf](https://www.paypalobjects.com/webstatic/ua/pdf/US/en_US/infringementreport.pdf).

172. *Id.*



successfully sued Visa for breach of its terms of service in a Russian court.<sup>173</sup> The over-blocking was to the disadvantage of Russian users, where the content was in fact legal, and also to the detriment of the payment processors who were held liable for the denial of service.

Another recent example of unilateral denial of service is PayPal's announcement that it would no longer be processing payments on behalf of companies offering Virtual Private Network (VPN) services, on the assumption that such companies enable copyright infringement.<sup>174</sup> The decision further illustrates the problem of over broadness of unilateral payment blocks for merchants and, in this instance, for their end consumers. PayPal is blocking payments to VPN providers, citing the terms of its Acceptable Use Policy. VPNs enable users to appear as though they are accessing the Internet from a different physical location. Like peer-to-peer file sharing, VPNs are known in the media for their illegal purposes, but they also have useful applications for legal conduct. Copyright holders lament the use of VPNs to evade geo-blocking of content. For example, a VPN could be used to view TV programming that is not licensed in the viewer's home country. However, the same geo-blocking evasion that makes VPNs such a scourge to rights holders is being challenged in the European Union as an often-unjustified restriction on cross-border e-commerce.<sup>175</sup> The decision to block payment services to VPN merchants ignores potentially valuable uses of VPNs where users want to keep their location private. The classic example is dissident political actors who want to mask their location to avoid persecution, but a more mundane and potentially legal application might be engaging in cross-border shopping. It is also conceivable that a company offering VPN services could also be offering other services for which it would no longer be able to accept PayPal payments. The payment block based on the offering of VPN services may thus be overly broad, impacting legal conduct to the great disadvantage of the merchants and users of their services.

---

173. The judgment was a pyrrhic victory for AllofMP3.com, given that the site shut down in the interim when the U.S. Trade Representative convinced the Russian government to make the site illegal through an amendment to Russian law. Robert Mackey, *The Day the Russian Music Service Died?*, N.Y. TIMES (Dec. 21, 2006, 7:54 AM), <https://thelede.blogs.nytimes.com/2006/12/21/the-day-the-russian-music-service-died/>.

174. Apparently without warning, PayPal stopped processing payments for the Canadian company UnoTelly, a supplier of VPN and SmartDNS services. Glyn Moody, *PayPal Blocks VPN, SmartDNS Provider's Payments Over Copyright Concerns*, ARS TECHNICA (Feb. 5, 2016), <http://arstechnica.com/tech-policy/2016/02/paypal-blocks-vpn-smartdns-providers-payments-over-copyright-violations/>.

175. Council of the European Union Press Release 692/16, Geo-blocking: Council Agrees to Remove Barriers to E-Commerce (Nov. 28, 1016), <http://www.consilium.europa.eu/en/press/press-releases/2016/11/28-geo-blocking>.

## II. EVALUATING OPTIONS FOR THE LEGAL TREATMENT OF ONLINE PAYMENT PROCESSORS: EFFICIENCY AND FAIRNESS CONSIDERATIONS

The theme across this discussion is that copyright holders are pushing hard to vindicate their rights online. All indications point toward payment processors as their target: the cases discussed above, the recent legislative proposals, and the resulting industry self-regulation. As this push continues, policy and lawmakers could either (1) allow the continued slow evolution of common law liability and the self-regulation of online payment processors, or (2) intervene more purposefully with a statutory DMCA-like safe harbor extended to some or all payment processors. The latter would involve an optional trade, in which payment processors who block infringing sales receive statutory protection from secondary liability. Both options are evaluated in this section based on the criteria of efficiency and fairness.

Whether to impose secondary copyright liability is often discussed in terms of maximizing efficiency. Authors suggest liability should be imposed where it minimizes various costs and maximizes the benefits to society overall.<sup>176</sup> In more specific terms, one author suggests “optimal digital copyright policy . . . would do two things: deter technological innovators as little as possible and permit cost-effective enforcement of copyright in the digital environment.”<sup>177</sup>

Efficiency of copyright enforcement certainly seems to underlie calls for secondary infringement liability of online intermediaries. Direct copyright suits against individual online infringers tend to be costly and ineffective, because infringers are so numerous, dispersed and hard to track down.<sup>178</sup> By the time the wheels of justice turn, the infringers have set up new, transient online shops, creating a “whack-a-mole” game for rights holders.<sup>179</sup> Even when a remedy is obtained, it may be small relative to litigation costs and difficult to enforce in practice if the infringer’s operations are outside of the U.S. In *Visa*, Judge Kozinski’s dissent echoes these considerations; he attributes cases like *Fonovisa*, *Aimster*, *Grokster*, and *Amazon* to the fact that

---

176. See, e.g., Haskel, *supra* note 80, at 423 (“One of the main purposes of secondary liability is to stop infringement at the least cost to society.”); Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003) (proposing an assessment where contributory copyright liability is determined based on the cost of direct infringement, the benefits of other lawful use, the cost of modifying behavior and the efficient gains from liability); Hogberg, *supra* note 39, at 918 (“Contributory Infringement . . . As with vicarious liability, the dominant mode of theoretical analysis of enterprise liability has traditionally been based on economic efficiency rather than fairness.”).

177. Lemley & Reese, *supra* note 20, at 1350.

178. See Blevins, *supra* note 33, at 1871; Haskel, *supra* note 80.

179. See, e.g., *Equustek Solutions Inc. v. Google, Inc.*, 2015 BCCA 265 (Can. B.C.), leave to appeal to SCC granted, 2017 SCC 34.

“direct infringers are sometimes too ubiquitous, too small, or too difficult to find.”<sup>180</sup>

Third parties—like ISPs, search engines, and payment processors—are bottlenecks whose control leaves them well positioned to reduce infringement at a lower cost, faster, and more easily than other stakeholders.<sup>181</sup> Judge Kozinski refers to payment processors as having “ready means” to stop the infringing conduct through simple measures.<sup>182</sup> The higher up the supply chain a copyright holder can target, the less the administrative or litigation burden there is to enforce rights, because there are fewer parties involved and greater impact on downstream users.<sup>183</sup> From a rights holder’s perspective, cutting off payment mechanisms is even more effective than seeking to control content through multiple ISPs or search engines. A payment block can quickly shut down the entirety of the illegal operator’s business, not just one or two webpages like a DMCA notice. From this perspective, the Payment Processor Agreement seems like an efficient centralized notice-and-blocking system, saving the rights holder from chasing each end user who is infringing, or even each payment intermediary, in separate litigation.

But the Payment Processor Agreement is far from the only online copyright enforcement system. As described for PayPal above, many payment processors also have unilateral blocking-request systems. As voluntary agreements and such unilateral policies proliferate, their complexity and patchiness raise efficiency and effectiveness questions. The American Bar Association’s Intellectual Property Section argues the emerging voluntary system is creating large administrative burdens on rights holders who seek vindication. Similar sentiments were expressed in the House Judiciary Committee hearings on copyright law reform, where one commentator characterized the voluntary agreements as simply “impos[ing] another layer of notifications.”<sup>184</sup> The problem seems likely to worsen in the future as payment processors sense their rising risk of secondary liability and respond with more voluntary policing. In comparison, the implementation of a legislated DMCA-like solution could offer greater uniformity, streamlining notice and takedown in a manner that reduces the administration and costs to the benefit of rights holders.<sup>185</sup> Since payment processors are on the receiv-

---

180. *Visa*, 494 F.3d at 823 (Kozinski, J., dissenting).

181. *See, e.g.*, Lemley & Reese, *supra* note 20, at 1349 (“The high volume of illegal uses, and the low return to suing any one individual, make it more cost-effective to aim litigation at targets as far up the chain as possible”).

182. *Visa*, 494 F.3d at 816 (Kozinski, J., dissenting).

183. *See*, Lemley & Reese, *supra* note 20, at 1349.

184. *Section 512 of Title 17, Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 97 (2014) (statement of Paul Doda).

185. ABA WHITE PAPER, A CALL FOR ACTION FOR ONLINE PIRACY AND COUNTERFEITING LEGISLATION *supra* note 124, at 71 (“Absent implementation of new legislation that cre-

ing end of the patchwork of rights holder notifications, streamlining into a single, legislated regime could improve efficiency for them as well.

The other major inefficiency of the *status quo*—self-regulation with emerging liability risk—is its potential for over-blocking of online commerce. This is a problem inherent in indirect liability lawsuits, which tend to “sweep together both socially beneficial and socially harmful uses of a program or service.”<sup>186</sup> As *Grokster* illustrates, the courts are not well-suited to design remedies at common law that enable even recognized non-infringing uses to continue. This is exacerbated by the Payment Processor Agreement and Rogue Block system, which encourage over-blocking of services. As discussed above, this industry self-regulating regime takes a rightsholder centric stance that enables blocks even for non-infringing transactions and merchants. Even if the merchant provides evidence of non-infringement or proceeds to litigation, the payment processor can still block the services and request indemnity from the rights holder.<sup>187</sup> The SOPA/PIPA bills suffered from the same over-blocking malady, requiring mandatory service blocks for websites with potentially non-infringing content.

Any over-blocking occurring in the current system creates inefficiency when it prevents legitimate, non-infringing transactions. Even worse, when a new business model tests the boundaries of established copyright jurisprudence—as *Grokster* and *Napster* did, and as VPNs may be doing now—it can be stymied by an inability to obtain payment services. In the face of uncertain copyright infringement liability, companies like PayPal may refuse services to business like VPN providers, whose business facilitates both illegal and legal conduct.

A DMCA-like legislative exception for payment processors could remedy some of the over-blocking inefficiency of the current approach. By (1) tailoring blocks to focus more specifically on illegal transactions or repeat offenders, as discussed in the next section proposing initial considerations for the design of a safe harbor and (2) creating more robust merchant protections, such as effective counter-notice or delayed blocking, to allow time for merchant challenges. A legislative solution could expressly clarify when payment processors are not liable. Like the DMCA, it could reduce monetary risks for payment processors who process transactions of indeterminate legality by restricting remedies to injunctive relief.<sup>188</sup> By clarifying the scope of liability and limiting remedies in these ways, a legislative exception could

---

ates greater uniformity among such initiatives, the burden that falls on copyright owners will only continue to grow, as new technologies rapidly evolve beyond the scope of protections and safe harbors currently covered by the DMCA, and which may make policing efforts less centralized and more expensive.”).

186. Lemley & Reese, *supra* note 20 at 1350.

187. Payment Processor Agreement, *supra* note 143 at sec. 11.

188. 17 U.S.C. § 512 (j) (describing the rules for applications for injunctions against online service providers).

reduce the uncertainty that drives inefficient over blocking, such as denials of service to innovative business models.

In addition to efficiency, several authors also discuss “fairness” as a theoretical basis for the imposition of secondary infringement liability.<sup>189</sup> This trends to encompass both procedural fairness in the notice and blocking processes and substantive fairness in who bears the burden of action.

Procedural fairness considerations might include the right of merchants to dispute allegations of copyright infringement in a timely manner, either before or after a payment blockade is imposed. They might also encompass consideration of who bears the initial power to decide that a payment block will be imposed and whether there is any unbiased ultimate oversight of blocking decisions.

Substantive fairness considerations might include correlating burden with benefit in the imposition of liability. If third parties benefit financially from the infringement of others, some argue that party should bear a correlating burden of policing against the related infringement. Judge Kozinski’s dissent in *Visa* takes this tack, objecting to payment processors “collecting billions for sellers of stolen merchandise; in a very real sense, they [payment processors] profit from making piracy possible.”<sup>190</sup> This contributes to Judge Kozinski’s conclusion that Visa and MasterCard should be liable. From this substantive fairness perspective, the argument would be that it is unjust to allow intermediaries to profit from piracy if they are well positioned to stop it. A further question is whether in exchange for assuming that proportionate policing obligation, some corresponding benefit, such as liability protection, would also be fair.

Current voluntary systems seem to fall short on measurements of procedural fairness for merchants. The Payment Processor Agreement was created by copyright owners and intermediaries and has predictably oriented the systems toward rights holders and blunt blocking of services. The payment processors hold the power to decide whether content is infringing, with no judicial backstop as there is under the DMCA. Professor Annemarie Bridy observes that the Payment Processor Agreement scheme “substitutes the hurried judgment of a participating intermediary for the more deliberate judgment of a court,” leaving this approach wanting on procedural fairness.<sup>191</sup> There is minimal recourse for merchants to challenge decisions, and experi-

---

189. MacCarthy, *supra* note 82, at 1055 (arguing normative considerations of fairness should be taken into account, in addition to efficiency, when determining whether to impose secondary infringement liability); Hogberg, *supra* note 39, at 919 (discussing fairness and culpability as concerns of contributory copyright liability, along with economic efficiency); Bridy, *supra* note 4, at 1560 (discussing online payment blockade from a fairness perspective); Blevins, *supra* note 34, at 1871–72 (discussing how the imposition of secondary liability promotes fairness by imposing costs on those who benefit from the infringement).

190. *Visa*, 494 F.3d at 816 (Kozinski, J., dissenting).

191. Bridy, *supra* note 4 at 1560.

ence to date shows merchants rarely make use of the recourse that is afforded to them.

Although the DMCA has faced criticism for promoting over-takedown of content, it offers at least some user rights protection through judicial oversight. Recent decisions encourage fair use, and illustrate how this oversight protects users' rights to a greater extent than voluntary systems with no neutral arbiter.<sup>192</sup> The same features of the DMCA-like system that could reduce over-blocking from an efficiency perspective, discussed above, would also improve fairness for merchants by encouraging more proportionate blocking of services.

Existing voluntary systems also seem substantively unfair for payment processors. Payment blocks, whether purely unilateral or pursuant to the Payment Processor Agreement, impose costs and obligations on payment processors akin to that of legislated notice and takedown under the DMCA, yet fail to offer the equivalent legal assurances against secondary copyright infringement liability of the DMCA. Reviewing and actioning notices for payment blocks inevitably consumes business resources of online intermediaries. As early as 2004, eBay was already spending \$20 million each year on tools to promote trust and safety on its website through a department with 4,000 employees, 200 of whom "focus exclusively on combatting infringement."<sup>193</sup> The resources dedicated to voluntarily minimizing infringement have no doubt skyrocketed since then and are similarly incurred by other online payment processors. Yet the protections from secondary liability are tenuous under the Payment Processor Agreement. It is not clear that under a DMCA-like regime the expenditures would be less, but at least the efforts would be in exchange for legislated secondary liability protections that eliminate the potential for monetary damages.

Finally, when the DMCA is involved in litigation, it arguably influences upward the standard for the conduct that meets certain elements of secondary copyright infringement, such as knowledge. A legislative exception could have the same influence in cases against payment processors. This is an added advantage to the DMCA-like option for online payment processors as they face secondary infringement jurisprudence edging toward inclusion of their business models.

Overall, a DMCA-like legislative safe harbor approach seems preferable based on the criteria of efficiency and fairness. A single legislative approach would be more efficient than the existing patchwork of voluntary systems. It could help to reduce inefficient over-blocking of legitimate commerce and the accompanying unfairness for merchants. A DMCA-like option would

---

192. See e.g., *Lenz v. Universal Music Corp.*, 801 F.3d 1126 (9th Cir. 2015) (vindicating user rights by requiring that copyright holders consider the fair use doctrine in filing a takedown notice claiming copyright infringement).

193. *Tiffany (NJ) Inc.*, 600 F.3d at 98.

also offer payment processors stronger liability protection than the current voluntary systems, and perhaps even influence upward the legal standards for when their conduct would trigger secondary copyright infringement. As an added advantage, the DMCA-like approach has been in existence since 1998, making it familiar to stakeholders.

Although the DMCA is far from perfect, it recognized early that a flourishing online marketplace required balance between reasonably efficient online copyright enforcement and the promotion of online commerce. Under the DMCA's influence, online commerce has become an essential part of the U.S. economy. But online payment processors are the keystone to continued success of e-commerce. The rising potential for secondary copyright liability of online payment processors, recent legislative proposals, and questionable voluntary systems all suggest it is time to bring a similar balance to copyright enforcement against these intermediaries.

### III. INITIAL CONSIDERATIONS IN THE DESIGN OF AN ONLINE PAYMENT PROCESSOR SAFE HARBOR FOR THE FUTURE

The DMCA experience over the last nearly twenty years provides valuable insight into areas of effectiveness and flaws.<sup>194</sup> The precise contours of a notice and payment blocking regime for payment processors could easily be the subject of another paper, but the following considerations will need to be taken into account at an early stage.

There are logical changes to the DMCA regime that would clearly be required to "fit" the safe harbor concept to online payment processors. For example, payment processors benefit financially from infringing sales, which seems likely to make them ineligible under the DMCA safe harbor exclusion of intermediaries who "receive a financial benefit directly attributable to the infringing activity."<sup>195</sup> The DMCA's financial-benefit criteria would have to be modified in a safe harbor applicable to payment processors.

By far the greatest substantive challenge is designing a safe harbor that balances the blunt nature of a payment blockade. As the contentious SOPA/PIPA regimes illustrate, both infringing and non-infringing transactions can occur on the same website or on different websites of the same merchant, yet all are impacted by a refusal to provide payment services to the merchant. This raises concerns about the inefficiency and broader social costs of over-blocking legitimate e-commerce. It may even go so far as to implicate the free speech and open-Internet concerns that sparked outrage over SOPA/

---

194. The current consultation by the Copyright Office on section 512 of the DMCA could also provide some unique insights into modifications that could apply to the design of a payment processor regime. *See generally* Section 512 Study: Notice and Request for Public Comment, *supra* note 8.

195. *See* 17 U.S.C. § 512(d)(2).

PIPA. To introduce a successful safe harbor regime for payment processors, some form of tailoring at a process and technical level is required to balance the potential blockage of non-infringing transactions. Three possible approaches to this tailoring are canvassed here: a notice-and-notice approach, a “critical volume” approach, and a three-strikes approach.

The DCMA regime has faced criticism for promoting over-takedown, where non-infringing content is removed simply because it is the easiest response for intermediaries.<sup>196</sup> One proposal put forth to remediate this issue in the DMCA is delaying takedown to allow time for counter notice. Rather than the current DMCA approach of immediate takedown upon notice from the rights holder, with the potential for later “put-back” of the content if a counter notice is sent, the proposed change would delay takedown to provide the subject of the notice with a chance to respond (called a “notice-and-notice” approach). A similar process for the regime applicable to payment processors could improve, although not fix, the over-blockage problem. It would give merchants the chance to provide specifics in their counter notice about their business, allowing the block to be tailored or declined by the payment processor (assuming the technical feasibility of such tailoring). The challenge with this approach is merchants would self-identify their infringing activity. Although evidence to refute the infringement claim could be required for a valid counter notice, it seems likely that the more egregious an offender, the more likely they are to provide dishonest information on infringement in their counter notice. This would undermine the effectiveness of the system to at least some extent.

Another possible approach to reduce over-blockage of payment processing is to implement a block only when a critical threshold of a website’s content appears to be infringing. When a rights holder can show that a website is predominantly engaging in sales of infringing goods, a payment block could be imposed. As Professor Mark Lemley observes, the level of infringement in the seminal cases seems to fall on a continuum; in *Napster*, approximately 87-99% of the end use appeared to be infringing, whereas in *Grokster* the rough estimates were lower at around 75% infringing use.<sup>197</sup> A blocking system that could differentiate between the predominantly infringing sites and those with mixed use or predominantly non-infringing sales would reduce the concern over blocking legitimate e-commerce. This would be straightforward for websites like TheBagAddiction.com in *Gucci*, which exclusively sold infringing goods. If sites are in fact more mixed in the legality of their offerings, one challenge of this approach is potential gaming by merchants. For example, if seven out of ten products offered are infring-

---

196. See, e.g., HASKEL, *supra* note 80, at 435 (referring to a 2006 study by Urban & Quilter suggesting DMCA section 512 protections were tilted in favor of copyright holders and that allegedly infringing material was often taken down even when the infringement claim is suspect).

197. Lemley & Reese, *supra* note 20, at 1380–81.



ing, a merchant could add another three “dummy” non-infringing products that it never expects to sell, leaving the payment processor in the difficult position of adjudicating which sites are “predominantly” infringing.

Perhaps the most feasible idea is to tailor payment processing blocks based on a three-strikes approach pursuant to which only repeat offenders are punished with a full payment block. Initially, copyright holders could be required to give notice to a payment processor that identifies specific infringing items, just as specific content is identified in valid DMCA notices. If specific transactions are identifiable, the amount of those transactions could be clawed back by the payment processor. When a merchant reaches a certain number of incidents, based on actioned notices from copyright holder(s), the payment processor could escalate to impose a full payment processing block on the merchant. This approach is reminiscent of the DMCA requirement that intermediaries have a policy of terminating repeat infringers.<sup>198</sup> If anything, payment processors are better positioned than the online intermediaries already covered by the DMCA to track and communicate with merchants whose accounts are the subject of repeated copyright violation claims, making it more feasible to implement such a three-strikes approach in a manner that is fair to merchants.

In addition, there is a question as to the scope of the DMCA’s protection against secondary liability. Some cases treat the elements that disqualify an intermediary from the safe harbor—such as financial benefit and the right and ability to control—as being identical to the parallel elements of claims for contributory infringement and vicarious liability.<sup>199</sup> This approach means evidence that suffices to prove secondary liability necessarily also excludes the intermediary from the safe harbor protections, so the DMCA protects only from direct infringement liability. This Article is based on the more logical view that the DMCA protects from secondary liability because the thresholds for proving disqualification from the safe harbors are higher than that of which is required to show secondary liability. Since there is no current intimation of direct copyright infringement by payment processors when they process merchant transactions, to be useful a safe harbor would have to resolve this ambiguity in the DMCA model in favor of providing protection from secondary liability.

Lastly, a key consideration in designing a payment processor safe harbor is defining which intermediaries or technologies are covered. Each party in the payment chain has a different role, amount of knowledge, and technology. As *Gucci* illustrates, these roles vary widely. PayPal itself plays differing roles, as merchant of record to enable Visa and MasterCard payments, or

---

198. See, e.g., 17 U.S.C. § 512(i)(1)(A) (policy must provide “for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers.”).

199. See, e.g., *In Re Aimster Copyright Litigation*, 334 F.3d 643, 654 (7th Cir. 2003).

offering its own PayPal-branded online payment services. The distinctions could be important in determining the requirements imposed on an intermediary in order to qualify for a safe harbor.

Lessons can be learned here from the DMCA, where a major criticism is the static nature of the intermediary categories covered by the legislation. The types of online service providers covered are the main intermediaries that were in existence in 1998, at least in the minds of legislators. New intermediaries, like peer-to-peer file sharers and of course payment intermediaries, were left without safe harbor protection even though their inclusion might have been desirable from a policy perspective. Striving for a safe harbor that stands the test of time for payment processors is already of great importance as new technologies, like Bitcoin, emerge.<sup>200</sup> Bitcoin, and other virtual currencies, have no central intermediaries and would therefore pose distinct challenges in determining how and to whom a safe harbor would apply.<sup>201</sup>

#### CONCLUSION

Policing online copyright infringement is complex for all involved—copyright holders, online intermediaries, the courts, legislators, and merchants. Jurisprudence on secondary copyright infringement is reaching toward intermediaries that are increasingly tangential to the direct infringement, as rights holders seek new ways to battle rampant online violations. The reasoning in recent cases, when applied to online payment processors, suggests their business model puts them at a higher risk of secondary copyright liability than traditional credit card companies. Recently proposed legislation and industry self-regulation have also taken aim at the role of payment processors in reducing online copyright infringement.

This significant attention begs the question of whether online payment processors should be granted legislative protection from secondary copyright infringement liability. Other online intermediaries are provided with such protection under the DMCA, in exchange for their assistance in policing online infringement. DMCA-like safe harbors offer efficiency and fairness

---

200. Bitcoin is a virtual currency that relies on blockchain technology to operate, which involves public key encryption and a public ledger. Although Bitcoin is the poster child, there are an estimated 600 virtual currencies relying on similar technology, including the now defunct “Coinye,” which features Kanye West’s face. See *Gold Diggers Defeated: Kanye West Wins Legal Battle Against Digital Currency Coinye*, THE GUARDIAN (July 27, 2014), <http://www.theguardian.com/music/shortcuts/2014/jul/27/kanye-west-head-on-coinye-cryptocurrency>.

201. See generally Parker Higgins, *In the Silk Road Case, Don’t Blame the Technology*, ELECTRONIC FRONTIER FOUNDATION (Oct. 3, 2013), <https://www EFF.org/deeplinks/2013/10/silk-road-case-dont-blame-technology>. The distinction between PayPal and Bitcoin, one centralized and one decentralized, for payment processing, is reminiscent of the similar distinction drawn between Napster and Grokster, although both file sharing services were ultimately found outside the DMCA safe harbor.

advantages for merchants, online payment processors and copyright holders that make them preferable to the current gradual evolution of liability and industry self-regulation. The design of such safe harbors in practice raises complex considerations of scope and practical application that require further examination. With or without safe harbors, the evolution of secondary copyright infringement will continue to pose complex questions of balance between the robustness of e-commerce and the ability of copyright holders to vindicate their rights online.