Internet Service Provider Liability: Imposing a Higher Duty of Care

Wendy C. Larson*

INTRODUCTION

Today's Internet is exploding with creativity and innovation, and it has spurred new markets and industries in an unprecedented period of time.[1] Such progress is inevitably accompanied by intellectual property rights violations, particularly as the law struggles to keep pace with the exponential growth in technology. Moreover, online actors are becoming increasingly skilled at hiding their identities to evade responsibility. The service providers that these actors employ to host their Web sites, auction their domain names, provide their advertising content, process their payments, promote their businesses—and even hide their identities—have limited exposure to liability for their customers' actions. As a consequence, service providers have little incentive to cooperate with brand owners or to voluntarily identify trademark violations. In fact, such cooperation or voluntary participation may place service providers at a competitive disadvantage. Law and practice should be revised to create incentives for service providers to work with brand owners to effect the primary purpose of trademark law: preventing consumer confusion.

This Article identifies the types of online services most often involved in trademark violations. It provides a brief review of the current statutory framework and the evolution of the common law concerning liability of online service providers. Borrowing from the Digital Millennium Copyright Act and traditional tort concepts, this Article explores avenues for legislative change and the best practices to address the issues.[2]

Requiring a higher duty of care from online service providers will help minimize consumer confusion, protect brand owners and provide a more authentic online consumer experience. It will incentivize innovation and help to promote fair competition among service providers.

* Member, Pirkey Barber PLLC.

1. As of the date of this writing, the new generic top-level domains (gTLDs) have not yet launched (though a few are in their sunrise periods). This revolutionary development is sure to create many more trademark challenges not addressed here.

2. It should be noted that this Article merely touches on many issues that are subject to complex technological explanations and processes, and is intended to be a broad overview to spur further discussion and ideas.

I. DEFINING "INTERNET SERVICES"

In exploring how a service provider's duty could or should be heightened,[3] this Article first identifies and defines certain online services and how such services constitute or contribute to trademark violations. This is not an exhaustive list of the existing types of online service providers; however, it is intended to provide a significant sampling of the service providers that are most often involved in trademark abuses.[4] Moreover, as it may be unhelpful to confine a provider to the services suggested by its common name (e.g., a domain name registrar), since many service providers offer a wide array of additional, related services, this Article will focus on particular services rather than on provider identities. The Article will then examine whether each case calls for heightened liability.

A. ADDRESSING DIRECT LIABILITY: SERVICE PROVIDERS WITH HIGHER LEVELS OF AWARENESS AND/OR INVOLVEMENT

The first group of services to be discussed has the most direct role in, or highest awareness level of, trademark violations.

1. Domain Name Registration Services

Domain name registration service providers have been given a pass from the beginning. One court explained that liability does not attach to a registrar when its customer registers and uses an infringing domain name, because the registrar merely provides the "rote translation service" of converting a domain name into an IP address.[5] Indeed, the Anticybersquatting Consumer Protection Act (ACPA) provides explicit immunity for domain name registrars that perform the mechanical function of registering strings of letters selected by their customers, the domain name registrants.[6]

3. Of course, there is a duty of care at some level already. For example, while a domain name registrar is generally immune from statutory damages under the Anti-Cybersquatting Consumer Protection Act, it can fall within the purview of an injunction. *See, e.g.*, Gucci Am., Inc. v. Weixing Li, 10 CIV. 4974 (RJS), 2011 WL 6156936 (S.D.N.Y. Aug. 23, 2011) (issuing a preliminary injunction binding non-party ISPs); Tory Burch LLC v. Yong Sheng Int'l Trade Co., Ltd., No. 10-cv-09336 (S.D.N.Y. May 13, 2011).

4. This Article does not focus on search engine advertising (i.e., "keyword advertising"), as that practice has been highly litigated and the boundaries of liability appear to be fairly well defined. For that reason, and because some brand owners engage in the practice themselves, focusing energy on liability reform for that practice is not a significant priority for brand owners (and by extension, this practitioner author) at this time.

5. Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 985 (9th Cir. 1999).

6. *See* 15 U.S.C. § 1125(d)(1)(D) (2012) ("A person shall be liable for using a domain name under subparagraph (A) only if that person is the domain name registrant or that registrant's authorized licensee."); *see also id.* § 1125(d)(2)(D)(ii) ("The domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order."). Indeed, a recent Ninth Circuit decision affirmed that the ACPA did not create a claim for contributory cybersquatting against a registrar in its role as a registrar. Petroliam Nasional Berhad v.

This rationale may have made sense when the ACPA was enacted in 1999; at that time, domain name ownership existed on a much smaller scale, registration transactions were manually entered and cybersquatting was a sporadic problem. Today's reality is different: cybersquatters use software to automatically register expiring names on a massive scale,[7] they routinely use privacy services to shield their identities, and registrars have actual and repeated knowledge of their customers' bad faith domain name registration and use. For example, in a Uniform Domain Name Dispute Resolution Policy (UDRP) proceeding, the complainant is required to notify the domain name registrar that a complaint was filed against its customer.[8] The registrar, in turn, must lock down that particular domain name (i.e., "maintain the status quo"), so that the name is not transferred away while the proceeding is pending.[9] When the trademark owner prevails in the UDRP proceeding, the registrar is tasked with transferring the domain name from its customer to the complainant.[10] Consequently, the registrar has notice of the proceeding from the beginning and has actual knowledge of the bad faith findings against its customers.

To further illustrate this point, one domain name owner, Transure Enterprises, has 168 UDRP decisions against it (as of the date of this writing). Each of these 168 decisions lists the same registrar, Above.com.[11] In each of those proceedings, as explained above, the same registrar was necessarily involved and has actual knowledge of the bad faith finding against its customer. Yet Above.com apparently continues to provide registration services to the customer. Those 168 UDRP proceedings represent approximately $250,000 in administrative filing fees alone (not including associated attorney's fees).[12] Such ongoing activity is a waste of resources, and unfortunately, this is not an atypical example.[13]

GoDaddy.com, Inc., 737 F.3d 546, 548 (9th Cir. 2013).

7. *See, e.g.*, *Domain Grabber*, DOMAIN SOFTWARE, http://www.dnware.com/products/grabber/enom.php (last visited Mar. 1, 2014) (advertising "Domain Grabber" software).

8. *See, e.g.*, NAT'L ARBITRATION FORUM, NATIONAL ARBITRATION FORUM'S SUPPLEMENTAL RULES TO ICANN'S UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY 2 (2010), *available at* http://domains.adrforum.com/users/icann/resources/UDRP%20Supplemental%20Rules%20eff%20July%201%202010%20(final).pdf.

9. *See Uniform Domain Name Dispute Resolution Policy*, INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS ¶ 7 (Oct. 24, 1999), http://www.icann.org/en/help/dndr/udrp/policy.

10. *See id.* ¶ 3(b)–(c).

11. This number is based on searches on the National Arbitration Forum (NAF) and World Intellectual Property Organization (WIPO) databases. *See Domain Name Dispute Proceedings and Decisions*, NAT'L ARBITRATION FORUM, http://domains.adrforum.com/decision.aspx (last visited Apr. 1, 2014); *Search WIPO Cases and WIPO Panel Decisions*, WORLD INTELL. PROP. ORG., http://www.wipo.int/amc/en/domains/search (last visited Apr. 1, 2014).

12. *See* NAT'L ARBITRATION FORUM, *supra* note 8, at 10–11 (setting out the NAF's UDRP fee schedule); *see also Schedule of Fees Under the UDRP*, WORLD INTELL. PROP. ORG. (Dec. 1, 2002), http://www.wipo.int/amc/en/domains/fees/index.html (setting out WIPO's UDRP fee schedule).

13. The domain names at issue in the relevant UDRP decisions target different trademark owners. Consequently, even if one of the trademark owners were to bring an ACPA action and secure an injunction, such an injunction would presumably only prohibit the party from registering domain names that are identical or confusingly similar to brand owners' marks; it would not prohibit that cybersquatter from registering domain names that violate others' trademarks.

Heightening liability for registrars that continue to provide registration services for repeated UDRP or ACPA violators could be positive, not only for consumers and brand owners but also for more scrupulous registrars. Many domain name registrars have written policies that authorize them to terminate customer accounts if the accounts are used to violate others' rights.[14] However, registrars appear reluctant to enforce their own policies. This reluctance is likely attributable to a lack of incentives: if a registrar cuts off a customer account, that customer could then take its portfolio elsewhere, to the registrar's competitive disadvantage. Moreover, some registrars are themselves cybersquatters or appear to exist for the sole purpose of supporting cybersquatters.[15] Implementing a higher legal standard could level the playing field, incentivize better practices and potentially drive out bad actors altogether.

A higher legal standard for registrars would also incentivize registrants' good behavior. While the ACPA permits statutory damages of up to $100,000 per domain name,[16] brand owners may be reluctant to pursue such a resource-intensive strategy when they are unlikely to collect. Moreover, while the UDRP has its strengths, its remedies do not include injunctions or monetary penalties.[17] Thus, cybersquatters often do not face meaningful consequences for their violations. However, if a registrar were required to terminate repeated cybersquatters' accounts or else be subject to ACPA liability, the registrar would be more likely to comply. Registrars would also likely include indemnification provisions particular to such a circumstance in their policies. If such practices were implemented, a domain name registrant might be more inclined to use the account for legitimate purposes, monitor its automatically registered domain names, or—if the account is solely dedicated to cybersquatting—find a new side income.

2. Privacy Services

There is a lack of uniformity in practice and procedure when it comes to privacy services.[18] This inconsistency leads to confusion in the courts and UDRP decisions concerning the role and responsibility of domain name privacy services when a

14. *See, e.g.*, *Register.com Master Services Agreement*, REGISTER.COM (Jan. 28, 2014), http://www.register.com/policy/servicesagreement.rcmx ("Register.com reserves the right to . . . terminate . . . any and all Services without notice if . . . in Register.com's sole discretion, the Services are used, or to be used, in a manner that is improper, illegal, in contravention of any of the representations or warranties made by Customer herein, or would otherwise amount to a breach of this Agreement or the documents or policies it incorporates by reference."); *Web.com Acceptable Use Policy*, REGISTER.COM (Nov. 5, 2013), http://www.register.com/policy/acceptable_use_policy.rcmx (prohibiting use of domain name for misappropriation of another's trademarks).

15. *See, e.g.*, Dell Inc. v. BelgiumDomains, LLC, 07-22674-CIV, 2007 WL 6862342 (S.D. Fla. Nov. 21, 2007).

16. 15 U.S.C. § 1117(d) (2012).

17. *See Uniform Domain Name Dispute Resolution Policy*, *supra* note 9, ¶ 4(i).

18. Privacy services companies replace the actual identifying information of domain name owners in required public records. *See, e.g.*, *Privacy Protect*, ABOUT PRIVACY PROTECTION, http://privacyprotect.org/about-privacyprotection (last visited Aug. 27, 2014) (offering to replace mailing address, email address and phone number with alternate information).

domain name is used to violate others' trademark rights.

It is not always clear who controls the privacy service.[19] It is impossible to know from the records on the Whois database—a public list of all the domain names registered worldwide—whether a customer is associated with a domain name. Indeed, in some instances the privacy service or registrar has no customer at all and controls the domain name itself.[20]

Based on the author's professional experience, privacy services have responded in various ways to cease and desist letters regarding their use of associated domain names. Some of these responses include: (1) no response or action taken at all; (2) a response from the customer indicating that the complaint was forwarded to them by the privacy service; (3) revealing its customer's information to the trademark owner, but maintaining the privacy shield in the Whois record; (4) removing the privacy shield in the Whois record altogether; (5) refusing to take action without a subpoena or court order;[21] (6) an automated e-mail stating that some further step must be taken, such as submitting the objection online or in a different format, before the complaint will be considered and (7) providing "famous" brand owners with a special e-mail address for expedited access to the legal department. After ignoring a cease and desist letter sent by e-mail and being named in a subsequent lawsuit, one privacy service insisted that the objection should have been sent by postal mail to be considered.[22] Other privacy services require that objections be sent electronically and state that all postal mail will be refused.[23]

Also inconsistent are privacy services' responses when they are named as respondents or defendants in UDRP complaints or lawsuits. Upon being named as defendants, privacy services typically reveal their customers' information and expect to be dropped from the lawsuit, no matter how complicit with their customer they have been up until that point. In a UDRP proceeding, however, some privacy services will reveal their customers' identities,[24] while others go through the entire proceeding as the respondent.[25] Both approaches can be problematic.[26]

19. A variety of indistinct privacy service names appear in Whois records—including, for example, PrivacyProtect.org, Whois Privacy Protection Services, Whois Privacy Inc., Privacy Block, Domain Privacy Service, and Privacy Ltd.—with no apparent requirement of uniformity or express association with a registrar. *See, e.g.*, *WHOIS Information for Privacyprotect.org*, WHOIS LOOKUP, http://whois.net/whois/privacyprotect.org (last visited Mar. 11, 2014).

20. *See, e.g.*, Dell Inc. v. BelgiumDomains, LLC, No. 07-22674-CIV, 2007 WL 6862342 (S.D. Fla. Nov. 21, 2007).

21. *See, e.g.*, Complaint at 11, Dell Inc. v. Domains By Proxy, Inc., No. 1:07-cv-00895-SS (W.D. Tex. 2007) (noting that a privacy service responded that it would "consider the matter closed" until it received a subpoena).

22. The aforementioned situations are drawn from the author's practice.

23. For example, Privacyprotect.org's Web site states, "We DO NOT accept Postal mails. All postal mails sent to our PO Box address are rejected." PRIVACY PROTECT, http://privacyprotect.org/ (last visited Mar. 11, 2014).

24. *See, e.g.*, Jaguar Cars Ltd. v. Domains By Proxy, LLC, No. FA1212001477048 (Nat'l Arbitration Forum Feb. 11, 2013), *available at* domains.adrforum.com/domains/decisions/1477048.htm.

25. *See, e.g.*, Cerberus Capital Mgmt., L.P. v. Domain Privacy Serv., No. FA1310001525549 (Nat'l Arbitration Forum Nov. 25, 2013), *available at* domains.adrforum.com/domains/decisions/1525549.htm.

26. For example, when a privacy service does not reveal its customer's information, there is no

Despite the general immunity granted to domain name registrars, privacy services have been held directly responsible for their users' violation of trademark rights under at least the UDRP and the ACPA.[27] The Internet Corporation for Assigned Names and Number's (ICANN's) 2013 Registrar Accreditation Agreement (RAA) would appear, at least in theory, to support such ongoing findings of liability. RAA Section 3.7.7.3 states:

> "A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it discloses the current contact information provided by the licensee and the identity of the licensee within seven (7) days to a party providing the Registered Name Holder reasonable evidence of actionable harm."[28]

However, the 2013 RAA falls short of implementing clear, uniform standards for privacy services. Currently, the applicable terms seem only to require that privacy services have contact information on their Web sites in the event of privacy or proxy server abuse, and that the privacy services outline what their policies are (without guidance or requirements of what those policies should include).[29] ICANN should require greater uniformity in practice. For example, privacy services could be required to have two separate points of contact: one for contacting the customer directly, and one to complain to the privacy service about the customer. This information should be in the Whois record and should, at minimum, include e-mail addresses. Upon receiving an objection from a trademark owner, in compliance with RAA Section 3.7.7.3, the privacy service should promptly reveal its customer's information to the trademark owner so that the parties may directly address the issue.

3. Parking Page Services

A parking page (also known as a pay-per-click site, PPC site, link farm or monetized parking page, among other names) is often created by the domain name

way to know whether there might be more issues, and no record of bad faith registrations is built. On the other hand, when a privacy service reveals its customer's information, particularly when there are multiple domain names and multiple customers at issue, a brand owner may be forced to revise and re-file its UDRP complaint, resulting in higher costs. Baylor University v. Domains by Proxy, Inc., No. FA0802001145651 (Nat'l Arbitration Forum May 26, 2008), *available at* domains.adrforum.com/domains/decisions/1145651.htm.

27. *See, e.g.*, *id.*; Baylor University v. Moniker Privacy Servs., No. FA1012001361618 (Nat'l Arbitration Forum Jan. 17, 2011), *available at* domains.adrforum.com/domains/decisions/1361618.htm; Solid Host, NL v. Namecheap, Inc., 652 F. Supp. 2d 1092, 1105 (C.D. Cal. 2009) (denying a motion to dismiss against a registrar providing privacy services and holding that "[15 U.S.C.] § 1114(2)(D)(i) was not intended to shield registrars from liability for actions outside their core function as registrars."); Freelife Int'l Holdings, LLC v. Domains By Proxy, Inc., No. FA0811001232485 (Nat'l Arbitration Forum Jan. 30, 2009), *available at* domains.adrforum.com/domains/decisions/1232485.htm.

28. *See 2013 Registrar Accreditation Agreement*, INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#privacy-proxy (last visited Mar. 11, 2014).

29. *See id.*

registrar in partnership with an advertising content provider.[30] The domain name registrant may or may not share with the parking service provider in the revenue generated by the parking page.[31] The advertising on the parking page is often generated by the terms in the domain name.[32] For example, as of this date, the parking page for the domain name columbiauniversity.co displays advertising for ITT Tech and online university degree programs, services obviously related to those offered by Columbia University in connection with its "Columbia University" mark. Posting a parking page on a newly registered domain name is a widespread and often automated process.[33]

When challenged for offering parking page services, domain name registrars have sought to invoke the protections of the ACPA's immunity provision. However, courts so far have rejected this defense, noting that parking page services go beyond simply registering domain names.[34]

Furthermore, at least one court recently found that a registrar, GoDaddy.com, was the domain name owner's "'Authorized Licensee' for purposes of ACPA liability" and that the registrar "'uses' and 'traffics in' domain names in its Parked Pages Program" in violation of the rights of the plaintiff, the Academy of Motion Picture Arts and Sciences.[35] Significantly, this decision clarifies that a parking page provider may be directly liable under the ACPA, which carries monetary penalties of up to $100,000 per domain name.[36] As registrars post parking pages as a matter of course across millions of domain names, the potential liability is significant.

The trend recognizing that parking page providers may be directly liable under the ACPA presents an opportunity for innovation. The engineering and licensing of blocking technology could allow service providers to continue providing parking pages but to screen such pages, in order to prevent pages from being posted for domain names that contain trademarks. Indeed, the plaintiff in *Academy of Motion Picture Arts and Sciences v. GoDaddy.com, Inc.* alleged that GoDaddy has applied for a patent for such filtering technology.[37] As such technology becomes available, courts will likely come to expect a higher standard of care from service providers.[38]

30. *See, e.g.*, Vulcan Golf, LLC v. Google Inc., 726 F. Supp. 2d 911, 913 (N.D. Ill. 2010).

31. *Id.*

32. *Id.*

33. *See, e.g.*, *id.*

34. *See, e.g.*, Solid Host, NL v. NameCheap, Inc., 652 F. Supp. 2d 1092, 1106 (C.D. Cal. 2009) (denying a registrar's motion to dismiss and holding that "NameCheap's status as an accredited registrar does not shield it from liability in cases where it did not act as a registrar"); *see also* Transamerica Corp. v. Moniker Online Servs., LLC, 672 F. Supp. 2d 1353, 1366 (S.D. Fla. 2009) (denying a registrar's motion to dismiss based on allegations that the registrar profited from its parking page activities in connection with the infringing domain names).

35. Acad. Motion Picture Arts & Scis. v. GoDaddy.com, Inc., No. 10-cv-3738, at *28 (C.D. Cal. June 21, 2013).

36. 15 U.S.C. § 1117(d) (2012).

37. Complaint at 10, Acad. Motion Picture Arts & Scis. v. GoDaddy.com, Inc., No. 10-cv-3738 (C.D. Cal. May 18, 2010). However, if the technology only screens trademarks after notice from a brand owner, rather than before such pages are posted, it may not protect a registrar from direct liability.

38. In medical malpractice law, for example, doctors are held to a greater standard of care as

However, service providers will not be incentivized to develop such technology if its existence could subject them to greater liability. Consequently, more courts may need to follow the *AMPAS v. GoDaddy* approach before the practice is changed.

4. Advertising Content Service Providers for Parking Pages

As noted above, a parking page is often posted by the domain name registrar in partnership with an advertising content provider. The advertising content provider contracts with individual advertisers and then supplies such advertisements, on an aggregated basis, to the parking page provider. Unlike the parking page providers, it can be difficult to ascertain the identity of the advertising content provider.

Like parking page providers, advertising content providers may be directly liable under the ACPA. In the Northern District of Illinois, Vulcan Golf sued Google and many other Internet service providers for violations of the ACPA, based on each of the parties' role in the provision of parking pages.[39] In a motion for summary judgment, Google argued that its part in the process did not fall within the scope of the ACPA.[40] The court disagreed, finding that Google could be a licensee of the registrant pursuant to 15 U.S.C. § 1125(d)(1)(D), and that Google's actions could be found to meet the "traffics in" element of 15 U.S.C. § 1125(d)(1)(E).[41]

It would appear that the implementation of blocking technology by the parking page providers, as discussed above, might moot the issue of liability for advertising content providers. Alternatively, advertising content providers could independently develop and implement such technology.

B. CONTRIBUTORY LIABILITY: SERVICE PROVIDERS WITH INDIRECT INVOLVEMENT IN TRADEMARK VIOLATIONS

The common proposal at the conclusion of this section concerns a variety of service providers, including domain name hosting services, online retailers, financial intermediaries, social media sites and domain name auction service providers. The proposal finds its origin in the Supreme Court case *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.*[42] The Court held that if a manufacturer or distributor intentionally induces another to infringe a trademark

research improves and technology advances. While it may have been common practice for doctors in the 1890s to prescribed cocaine for a teething baby, for example, doctors today would stripped of their licenses, or worse, for doing the same. *See, e.g.*, *Cocaine Tooth Drops, Morphine Teething Syrup and Other Victorian Quack Cures*, Telegraph, http://www.telegraph.co.uk/health/healthpicturegalleries/9519906/Cocaine-tooth-drops-morphine-teething-syrup-and-other-Victorian-quack-cures.html (last visited Feb. 14, 2014). We have higher expectations today because of better research and technology, and the duty of care is heightened as a result.

39. Vulcan Golf, LLC v. Google Inc., 726 F. Supp. 2d 911 (N.D. Ill. 2010).
40. *Id.* at 917–21.
41. *Id.*
42. Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844 (1982).

or—as is more common in the practices described below—continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer or distributor is contributorily responsible for any harm resulting from the deceit.[43] The *Inwood* standard was later applied to services in the Seventh Circuit and to online services in the Ninth Circuit.[44] When the primary infringer supplies a service rather than a product, a court must "consider the extent of control exercised by the defendant over the third party's means of infringement."[45]

1. Domain Name Hosting Services

The *Inwood* standard was applied specifically to Web site hosting services in *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*.[46] In that case, Louis Vuitton repeatedly sent notices of infringement to the hosting service Akanoc and received no response.[47] In affirming a contributory liability finding against Akanoc, the Ninth Circuit found that the company "had direct control over the 'master switch' that kept the Web sites online and available."[48]

2. Online Retailers

The *Inwood* standard has also been applied to online retailers such as eBay. In the Second Circuit case *Tiffany (NJ) Inc. v. eBay Inc.*, the court applied *Inwood* but found that eBay was not contributorily liable for trademark infringement.[49] eBay had responded to Tiffany's specific notices of counterfeit products, and eBay had a robust anticounterfeiting policy and practice.[50] The court held that generalized knowledge that infringement was occurring was insufficient to trigger liability under *Inwood*, and that a brand owner has the burden of finding and raising specific instances of infringement to the service provider.[51]

3. Financial Intermediary Services

Similarly, *Inwood* has been applied to online financial services companies. In the Southern District of New York, Gucci sued financial companies offering credit card processing for a Web site selling counterfeit bags.[52] Gucci alleged that the

43. *Id.* at 854.

44. Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 983–84 (9th Cir. 1999); Hard Rock Café Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1149 (7th Cir. 1992).

45. Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788, 807 (9th Cir. 2007) (quoting *Lockheed Martin*, 194 F.3d at 984) (internal quotation marks omitted).

46. Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 658 F.3d 936, 942 (9th Cir. 2001).

47. *Id.* at 940–41.

48. *Id.* at 943.

49. Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 103–05 (2d Cir. 2010).

50. *Id.* at 98–100.

51. *Id.* at 107.

52. Gucci Am., Inc. v. Frontline Processing Corp., 721 F. Supp. 2d 228 (S.D.N.Y. 2010).

companies: (1) were aware that the Web site owners had difficulty finding credit card companies because they ran a "replica" business; (2) knew of consumer complaints concerning the quality of the products offered on the site and (3) should have known the products were not genuine based on their low prices.[53] The court denied the defendants' motion to dismiss, stating, "These . . . claims are enough to at least infer that [the credit card processor] knew or consciously avoided knowing that the counterfeit products were sold on [the Web site]."[54] The court further noted that for the credit card company to be held liable, it was not necessary that the company have the ability to shut down the Web site.[55] Rather, it was sufficient that the Web site was "functionally dependent" on the defendants.[56]

4. Domain Name Auction Services

Domain name auction services often list domain names that are clear violations of trademark rights.[57] Offering such names harms not only the trademark owners but also the auction service provider's customers. In the author's professional experience, after receiving a cease and desist letter, domain name registrants have reported that they purchased a clearly infringing domain name for a significant sum of money from an auction site, believing that the name must be legitimate if it was listed there. Of course, a brand owner can easily recover such a name in a UDRP proceeding. As the auction service provider profits from the sale of a clearly infringing name and typically disclaims all warranties as to any conflicting third party rights,[58] there appears to be little incentive for such companies to de-list or block such names.

5. Social Media Services

In the context of service provider liability, the services offered by a social media site are arguably similar to those offered by a hosting service company. Each offers server space for its customers' online content and directly controls the "master switch" to the site; in other words, it has the technical capability to remove the content. Consequently, while *Inwood* apparently has not been applied in any trademark lawsuits against social media sites, such application would be a natural extension of the Ninth Circuit's holding in *Louis Vuitton*.[59]

53. *Id*. at 250.
54. *Id.*
55. *Id.* at 252.
56. *Id.* at 253.
57. For example, the domain name Kodak.biz is listed with online domain marketplace Sedo for $1,500. *Search Domains: Kodak.biz*, Sedo, http://sedo.com/search/searchresult.php4?domain=kodak.biz&language=us (last visited Feb. 14, 2014).
58. *See, e.g.*, *Auctions Membership Agreement*, GoDaddy, https://www.godaddy.com/agreements/showdoc.aspx?pageid=dna_member (last visited Mar. 11, 2014).
59. For a discussion of the *Louis Vuitton* case, see *supra* Part I.B.1.

II. TWO-FOLD PROPOSAL CONCERNING CONTRIBUTORY LIABILITY: (1) IMPLEMENT NOTICE AND TAKEDOWN PROCEDURE AND (2) REQUIRE TERMINATION OF REPEAT OFFENDERS' ACCOUNTS

The Lanham Act could be amended to impose service provider liability in two circumstances. The first would mirror the *Inwood* standard, which would effectively manifest as a notice and takedown procedure similar to that included in the Digital Millennium Copyright Act (DMCA). In other words, a service provider with control over the infringing activity is immune from liability so long as it promptly responds to a trademark objection or to circumstances supporting a finding that the service provider should have been aware of the activity.[60] If the provider continues to supply services to its customer after receiving such notice, then it may be contributorily liable, consistent with the *Inwood* line of cases.

The second part of this proposal, similar to a provision in the DMCA, would attempt to address the problem of repeat infringers. The DMCA states that a service provider is entitled to the Act's safe harbor if, among other things, it "has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."[61] Commentators have complained of the vague language in this section of the DMCA (including "reasonably implemented," "appropriate circumstances" and "repeat infringers"), which has led to inconsistent and unhelpful decisions for rights holders.[62] Consequently, any amendment to the Lanham Act similar to this provision should be adopted only after careful consideration of the historical application of the DMCA, and should attempt to clarify the ambiguities. Without a real threat of a terminated account,[63] however, there is little incentive for infringers (particularly when they have been successful at remaining anonymous) to comply with trademark laws.

Amending the Lanham Act to codify *Inwood*, as it has been developing in the case law, would create uniformity across circuits and clarify that the contributory liability standard is not only applicable to hosting services, online retail services and financial intermediary services, but to all online service providers.

60. This would be consistent with, for example, the *Gucci* case. *See* Gucci Am., Inc. v. Frontline Processing Corp., 721 F. Supp. 2d 228 (S.D.N.Y. 2010). For further discussion of *Gucci*, see *supra* Part I.B.3.

61. 17 U.S.C. § 512(i)(1)(A) (2012).

62. *See, e.g.*, U.S. PATENT & TRADEMARK OFFICE, DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COPYRIGHT POLICY, CREATIVITY, AND INNOVATION IN THE DIGITAL ECONOMY 59–60 (2013), *available at* http://www.uspto.gov/news/publications/copyrightgreenpaper.pdf.

63. While many service providers reserve for themselves the right to terminate accounts when their customers violate third parties' rights (*see, e.g.*, *supra* note 14), actual termination of such accounts appears to be rare.