9-22-2010

Unmasking the Mask-Maker: Domain Privacy Services and Contributory Copyright Infringement

Paulo André de Almeida
Loyola Law School Los Angeles

UNMASKING THE MASK-MAKER: DOMAIN PRIVACY SERVICES AND CONTRIBUTORY COPYRIGHT INFRINGEMENT

"Domain privacy services" are online services that protect the anonymity of their website-operating customers. Typically, the privacy service registers a domain name on behalf of its website-operating customer, and then leases the domain name back to the customer. The customer retains the right to use and control the domain, while the privacy service holds itself out as the true owner through the registrar's WHOIS database. Copyright-infringing website owners prefer this arrangement to avoid prosecution by forcing aggrieved copyright holders to first contact the listed privacy service, which typically refuses to reveal the identity of the alleged infringer. This Comment argues that privacy services which license domain names to known copyright infringers should be held secondarily liable on a contributory copyright infringement theory. Further, this Comment proposes a new model cease-and-desist letter warning privacy services that this licensing scheme likely violates ICANN rules as well as most privacy services' own "terms of service" agreements, and likely opens the privacy service to contributory copyright infringement liability.

I. INTRODUCTION

Imagine trying to operate a successful record label or movie studio in a world fraught with widespread illegal file sharing. Imagine that someone has created a website dedicated to distributing your company's content online for free without your permission. You run a domain ownership query on the unauthorized site at www.WHOIS.org—a phone book-like directory listing of all website operators—to find the name and e-mail address of the person running the site[1] so that you can issue your routine cease-and-desist letter.[2] Instead of displaying the site operator's contact information, the di-

1. Wikipedia, Whois, http://en.wikipedia.org/wiki/Whois (last visited Aug. 26, 2010) [hereinafter Wikipedia, Whois].

2. *See generally* Richard Keyt, *Internet Copyright Law: A Rat Pilfered My Web Site Cheese - What Do I Do?*, KEYTLAW, Nov. 9, 2002, http://www.keytlaw.com/Copyrights/cheese.htm.

rectory lists something called a "privacy service" as the site owner, and gives you the privacy service's contact information.[3]

You send numerous e-mail complaints to the privacy service, all of which are ignored, and you have no other way to contact the person running the unauthorized site. Your lawyer tells you that the privacy service is not intimidated by threats or demands of any kind, and the only way to obtain the identity of the person running the unauthorized site is to subpoena the privacy service's customer records, which requires filing an expensive lawsuit.[4] Meanwhile, new unauthorized sites have appeared on the Internet, and you simply cannot afford to issue a subpoena against every "private" infringer.[5] The privacy service stands between you and the biggest threat to your business—Internet piracy—and there is nothing you can do about it.

After Napster ushered in a culture of online file sharing, many copyright holders faced extinction unless they could successfully assume the burden of policing the Internet for copyright infringement.[6] Those media companies that could afford to hire teams of lawyers to enforce their copyrights developed anti-piracy programs[7] or outsourced the police work to private enforcement agencies.[8] Much of today's anti-piracy efforts focus on policing illicit uses of complex Peer-to-Peer and BitTorrent technologies,[9] but traditional client-server or website-based commission or facilitation of copyright infringement remains a problem for many copyright holders.[10] "Cyberlockers," such as Rapidshare, for example, are website-based file sharing services that allow users to post content for retrieval by others,

---

3. Domains By Proxy, How Private Registrations Work, http://www.domainsbyproxy.com/GetDBP.aspx (last visited Aug. 25, 2010) [hereinafter How Private Registrations Work].

4. *See* Domains By Proxy, Domains By Proxy Civil Subpoena Policy, http://domainsbyproxy.com/popup/subpoenapolicies.aspx (last visited Sept. 8, 2010) [hereinafter Domains By Proxy Civil Subpoena Policy]. *See generally* FED. R. CIV. P. 45.

5. *See* Domains By Proxy Civil Subpoena Policy, *supra* note 4.

6. *See generally* David Lieberman, *Piracy Pillages Music Industry*, USATODAY.COM, Apr. 8, 2002, http://www.usatoday.com/money/covers/2002-04-05-music-piracy.htm (warning that the music industry could collapse as a result of widespread illegal file sharing).

7. *See, e.g.*, Press Release, Universal Music Group, David Benjamin Named Senior Vice President, Anti-Piracy, Universal Music Group (July 15, 2002), *available at* http://www.universalmusic.com/corporate/news35192.

8. *See generally* BayTSP.com, Tracking, http://www.baytsp.com./services/tracking.html (last visited Aug. 24, 2010).

9. *See id.* (stating that an anti-piracy enforcement agency uses new technology to scan peer-to-peer and BitTorrent networks for infringing content).

10. *See* Posting of Vic to Code Confidential, http://vilabs.typepad.com/vilabs/2009/06/ubiquitous-cyberlocker-file-share-service-gets-fined.html (June 25, 2009, 16:41 EST).

often in exchange for a flat monthly or yearly fee.[11] Despite the relatively simple client-server technology relied upon by Cyberlockers, the sheer number and popularity of these types of sites makes online copyright enforcement very difficult.[12]

The Digital Millennium Copyright Act ("DMCA")[13] allows copyright holders to send a cease-and-desist letter called a "takedown notice" to suspected infringers or their Internet service providers ("ISP").[14] Recipients then have the opportunity to respond by removing the infringing content or challenging the allegation contained in the notice.[15] Part of a copyright holder's day-to-day enforcement includes sending takedown notices to website operators or their ISPs who commit or facilitate copyright infringement.[16] Today, the takedown notice procedure has become less burdensome with the help of digital fingerprinting and automated notice-and-takedown technology,[17] but infringers have become equally resourceful and have found ways to remain anonymous online.[18] When a copyright holder cannot determine the e-mail or physical address of a suspected infringer and cannot contact the infringer's ISP because of the use of anonymity services or software, the takedown procedure is useless.[19]

The Internet Coalition for Assigned Names and Numbers (ICANN) is a U.S. nonprofit corporation[20] that is widely regarded as the closest thing to a "government" of the Internet.[21] ICANN controls the top level domains of

---

11. *Id.*

12. *Id.*

13. Digital Millennium Copyright Act, 17 U.S.C. § 512 (2006).

14. *See id.* § 512(c)(1)(C).

15. *See id.* § 512(g)(1)–(3).

16. *See generally* David Krauets, *10 Years Later, Misunderstood DMCA is the Law That Saved the Web*, WIRED.COM, Oct. 27, 2008, http://www.wired.com/threatlevel/2008/10/ten-years-later (describing routine uses of the DMCA takedown procedure).

17. BayTSP.com, *supra* note 8.

18. *See* Wikipedia, Anonymizer, http://en.wikipedia.org/wiki/Anonymizer (last visited Jan. 30, 2010) (describing various technologies used to create anonymity and make Internet activity untraceable).

19. *See* Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (explaining that "[p]arties who have been injured by [copyright infringement] are likely to find themselves chasing the [anonymous] tortfeasor from Internet Service Provider (ISP) to ISP, with little or no hope of actually discovering the identity of the tortfeasor.").

20. ICANN, About, http://www.ICANN.org/en/about/ (last visited Aug. 24, 2010) [hereinafter ICANN, About].

21. *See generally* Kathleen E. Fuller, *ICANN: The Debate Over Governing the Internet*, 2001 DUKE L. & TECH. REV. 2 (2001), http://www.law.duke.edu/journals/dltr/ARTICLES/2001dltr0002.html (comparing ICANN to a government of the Internet).

the Internet (.com, .net) and sets policies regarding the sale of "parcels" of the Internet in the form of web domains.[22] ICANN delegates to "registrars"[23] the power to activate and sell domain names through an agreement called the Registrar Accreditation Agreement ("RAA").[24] Registrars sell the domain names to "registrants" or "registered name holders," who are the ultimate consumers and owners of the web domains.[25]

Currently, ICANN policy requires that all domain registrants make their personal information—including name and e-mail address—available in each registrar's publicly-accessible WHOIS database.[26] The RAA charges registrars with maintaining a complete and accurate WHOIS database as a condition of remaining an accredited seller of domain names.[27] This policy is widely criticized because spammers, data harvesters, and even stalkers can freely access the database to obtain any website owner's personal information.[28] On the other hand, the WHOIS database forces website owners to be accountable for their actions online and aids law enforcement in fighting cybercrime.[29] The WHOIS database is instrumental to intellectual property holders' enforcement of their rights because it allows them to identify infringers quickly and efficiently.[30]

In response to privacy concerns surrounding the WHOIS database, "domain privacy services" such as Domains By Proxy and WhoisGuard began offering anonymity protection service to website operators.[31] The service works as follows: the privacy service registers a domain name on behalf of its customer and then licenses control of the domain name back to

---

22. ICANN, About, *supra* note 20.

23. Registrars are wholesalers of domain names. Consumers purchase domain names from registrars such as Go Daddy. *See* GoDaddy.com, http://www.godaddy.com (last visited Sept. 14, 2010). *See generally* Wikipedia, Domain Name Registrar, http://en.wikipedia.org/wiki/Domain_name_registrar (last visited Sept. 12, 2010).

24. *See generally* ICANN, May 2009 Registrar Accreditation Agreement, http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm [hereinafter RAA].

25. *Id.*

26. *Id.*, §§ 3.3, 3.7.7.1; *see also* WHOIS Lookup, http://www.whois.net (last visited Sept. 14, 2010).

27. RAA, *supra* note 24, §§ 3.1, 3.3.

28. Wikipedia, Domain Privacy, http://en.wikipedia.org/wiki/Domain_privacy (last visited Sept. 14, 2010) [hereinafter Wikipedia, Domain Privacy].

29. *See* Wikipedia, Whois, *supra* note 1.

30. *See id*.

31. Domains By Proxy, About Domains By Proxy, http://www.domainsbyproxy.com/About.aspx?prog_id= (last visited Sept. 14, 2010) [hereinafter About Domains By Proxy]; *see also* WhoisGuard, http://www.whoisguard.com (last visited Sept. 14, 2010).

the customer for a fee.[32] The privacy service becomes the registrant and owner of the domain name, while the customer/licensee retains the rights to use and sell the domain name.[33] This licensing scheme is detailed in all privacy services' Terms of Service ("TOS") agreements with their customers,[34] and the purpose of the arrangement is to cause the privacy service's contact information—not the customer's—to appear in the registrar's WHOIS database.[35] This arrangement complies with ICANN rules because the privacy service is correctly named as the owner of the domain in the WHOIS database.[36] The end result is that the website operator cannot be identified through the WHOIS database and cannot be contacted directly by anyone except the privacy service.[37]

Many website owners have legitimate reasons for remaining anonymous, but others use the anonymity to operate infringing websites with impunity.[38] Copyright holders cannot send DMCA takedown notices to hidden infringers, and privacy services typically do not respond to allegations of infringement made by aggrieved intellectual property holders.[39] DMCA Section 512(h) allows copyright holders to send pre-litigation subpoenas to "online service providers" to compel release of their infringing customers' contact information,[40] however the section does not apply to services that do not store infringing content on their servers.[41] Domain privacy services

32. *See* How Private Registrations Work, *supra* note 3.

33. Domains By Proxy, Domain Name Proxy Agreement § 2, https://www.domainsbyproxy.com/policy/ShowDoc.aspx?pageid=domain_nameproxy (last visited Nov. 10, 2010) [hereinafter Domains By Proxy TOS].

34. *See, e.g., id.*; *see also* Namecheap, Inc., WhoisGuard Service Agreement § 1–2, http://www.namecheap.com/legal/whoisguard-agreement.asp (last visited Sept. 14, 2010) [hereinafter WhoisGuard TOS].

35. *See* How Private Registrations Work, *supra* note 3.

36. ICANN, FAQ's, http://www.icann.org/en/faq (last visited Sept. 7, 2010).

37. About Domains By Proxy, *supra* note 31.

38. Posting of Eric Goldman to Tech. & Mktg. L. Blog, http://blog.ericgoldman.org/archives/2009/05/ (May 28, 2009, 10:15:27 PST) (describing how an alleged cybersquatter used a privacy service to commit trademark infringement under the cloak of anonymity).

39. *See* Solid Host, NL v. Namecheap, Inc., 652 F. Supp. 2d 1092, 1098 (C.D. Cal. 2009) (quoting a defendant privacy service that stated "it would 'remain neutral'" in a dispute between an infringer customer and an aggrieved trademark holder); *see also* Domains by Proxy, Frequently Asked Questions, http://products.secureserver.net/products/domains_by_proxy/dbp_faq.htm#correspondence (last visited Sept. 14, 2010) (stating that Domains By Proxy merely forwards e-mail complaints to its customers) [hereinafter Domains by Proxy FAQ's].

40. *See* 17 U.S.C. § 512(h).

41. Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1233 (D.C. Cir. 2003).

are not subject to these subpoenas because they offer no such file storage functions.[42]

Seemingly, copyright holders seeking to enforce their rights against infringers who use privacy services are limited to either (1) requesting that the privacy service reveal an infringing customer in the name of fairness or (2) compelling release of the infringer's identity by subpoena through the discovery process.[43] The first option is tantamount to asking the privacy service to vitiate the only service that it provides—a request that would surely be ignored. The second option is untenable because it requires filing a costly lawsuit against every suspected infringer,[44] which requires a case-by-case analysis of whether discovery of an alleged infringer's identity violates his or her First Amendment right to remain anonymous.[45] Neither option provides any incentive for privacy services to stop harboring infringers or to monitor illicit use of their services.

Without other viable alternatives, an aggrieved copyright holder should consider bringing a contributory copyright infringement action against a privacy service for knowingly assisting certain customers in the commission of copyright infringement. A successful suit would set a valuable precedent for privacy services' joint liability for copyright infringement, which would deter privacy services from protecting infringers, and encourage them to monitor illicit uses of their services. Part II of this article explores the legal issues and arguments that would likely be raised in such a lawsuit.

Before filing a complaint, however, an aggrieved copyright holder should send a letter to the privacy service demanding release of the alleged infringer's contact information and warning of the legal consequences for knowingly assisting infringers. A strongly-worded letter containing clear evidence of the infringing activity should influence the privacy service to reconsider its privacy policy in the limited situation where a person's intellectual property rights are being violated. Part III of this article discusses the legal support for this "demand letter." Part V contains a sample de-

---

42. Wikipedia, Domain Privacy, *supra* note 28 (stating that domain privacy services solely provide private registration or "forwarding" services).

43. *See generally* FED. R. CIV. P. 45.

44. *Id.*

45. *See Columbia*, 185 F.R.D. at 578–80 (requiring a plaintiff seeking to discover the identity of a "Doe" defendant to (1) identify the defendant with enough specificity to allow the court to determine whether the defendant is a real person or entity who could be sued in federal court; (2) recount the steps taken to locate the defendant; (3) show that the action could survive a motion to dismiss; and (4) file a request for discovery with the court identifying the persons or entities on whom discovery process might be served). Variations of this test are used in different jurisdictions. *See* Solers, Inc. v. Doe, 977 A.2d 941, 951 (D.C. 2009).

mand letter that could be adapted and sent to a privacy service as a prelude to litigation.

Today, exposing infringers to liability requires exposing those who intentionally assist them as well. Privacy services and their customers should understand that the law strikes a balance between the right to anonymity and the protection of those harmed by its abuse.[46]

II. DOMAIN PRIVACY SERVICES THAT KNOWINGLY ASSIST CUSTOMERS IN THE COMMISSION OF COPYRIGHT INFRINGEMENT SHOULD BE FOUND LIABLE ON A THEORY OF CONTRIBUTORY INFRINGEMENT

A copyright holder filing an action against an anonymous infringer should also pursue any privacy service that knowingly assists the infringer using a theory of contributory liability. The copyright holder should file a complaint alleging a direct copyright infringement claim against the anonymous infringer as a "Doe" defendant,[47] and the privacy service should be named as an additional defendant and pursued on a claim of contributory copyright infringement.[48] Filing a lawsuit would allow a copyright holder to obtain the identity of the "Doe" infringer through issuing a subpoena in discovery.[49] However, a plaintiff must overcome a First Amendment hurdle before a court can compel release of an anonymous defendant's identity.[50]

On the merits of the case, contributory copyright infringement requires: (1) direct infringement by a third party[51] and that the defendant (2)

---

46. *See Solers*, 977 A.2d at 951 ("[W]e must strike a balance 'between the well-established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests . . . through the assertion of recognizable claims based on the actionable conduct of the anonymous, fictitiously-named defendant.'" (quoting Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001))).

47. *See* FED. R. CIV. P. 15(c)(3) (permitting plaintiff to amend defendant's name on complaint while retaining original filing date).

48. *See* FED. R. CIV. P. 20(a) (permitting joinder of defendants).

49. *See* FED. R. CIV. P. 45(a)(1)(D).

50. *See Columbia*, 185 F.R.D. at 578–80 (requiring a plaintiff seeking to discover the identity of a "Doe" defendant to (1) identify the defendant with enough specificity to allow the Court to determine whether the defendant is a real person or entity who could be sued in federal court; (2) recount the steps taken to locate the defendant; (3) show that the action could survive a motion to dismiss; and (4) file a request for discovery with the court identifying the persons or entities on whom discovery process might be served). This article assumes personal jurisdiction, and that the copyright holder has a strong infringement claim. So long as the plaintiff has a serious, non-frivolous claim, these requirements are likely satisfied, and the privacy service must comply with the subpoena.

51. Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir.

knowingly and (3) materially contributed to the direct infringement.[52] Contributory copyright infringement liability is not expressly provided for in the copyright statutes,[53] but the doctrine arose in the brick-and-mortar context, where absentee-landlords and flea market owners were held liable for the infringing activities of their patrons.[54] A defendant privacy service should be expected to vigorously dispute the "material contribution" element, as this case involves cyberspace intangibles such as domain names and Internet anonymity, which are not squarely addressed in the leading contributory infringement cases. In the 21st century, however, the distinction between real space and cyberspace is only minimally helpful, and the analysis turns on how directly or indirectly the secondary infringer assists the primary infringer.[55]

Two complete defenses to contributory copyright infringement have developed amid changes in technology: the DMCA Section 512(a) provides immunity for certain kinds of Internet service providers,[56] and the Supreme Court created a complete defense for makers of products capable of both infringing and non-infringing uses in the seminal *Sony-Betamax* case.[57] The latter defense protects makers of "staple article[s] of commerce" such as photocopiers, cameras, and recorders.[58] Privacy services should be expected to raise both of these defenses, as well as a third defense based on a First Amendment right to protect the anonymous speech of others.[59] However, the court should reject all of these defenses and im-

---

1971).

52. *Id.*

53. Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261 (9th Cir. 1996).

54. *See* Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 816 n.10 (9th Cir. 2007) (Kozinski, J., dissenting) ("It is true that [the absentee-landlord] cases were developed in a brick and mortar world . . . ."); *see also Fonovisa,* 76 F.3d at 264 (holding flea market owner liable for contributory copyright infringement because the infringing activity could not take place "without the support services provided by the [flea market] . . . .").

55. *See Perfect 10*, 494 F.3d at 796 ("The [Defendants] cannot be said to materially contribute to the infringement in this case because they have no direct connection to that infringement . . . ."); *see also id.* at 816 n.10 (Kozinski, J., dissenting) ("It is true that [the absentee-landlord] cases were developed in a brick and mortar world, but the distinction they draw between those who materially assist infringement (and are therefore liable) and those who are more remotely involved (and are therefore not liable) is equally important-perhaps even more important-in cyberspace than in real space.").

56. 17 U.S.C. § 512(a).

57. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 456 (1984).

58. *Id.* at 426.

59. *See Solers*, 977 A.2d at 950 (observing that anonymous Internet speech is protected by the First Amendment). The privacy service would likely have standing to assert a First Amendment right to remain anonymous on behalf of its customers. NAACP v. Ala. ex. rel. Patterson, 357 U.S. 449, 459 (1958); Va. v. Am. Booksellers Ass'n., 484 U.S. 383, 392–93 (1988) (allowing

pose liability for the reasons discussed below.

A. Direct Infringement by a Third Party

Contributory copyright infringement first requires direct infringement by a third party.[60] This article assumes that a copyright holder has a strong case of direct infringement against the underlying website operator, and will instead focus on the contributory liability of the privacy service. The main purpose of the lawsuit would be to create a precedent for privacy service liability in the copyright context, which would discourage privacy services from protecting customers who they know are abusing the service to commit infringement.

B. The Knowledge Requirement

The second element of contributory copyright infringement requires actual or constructive knowledge of the primary infringement.[61] Knowledge of specific infringement is not required.[62] To prove knowledge, the copyright holder must "provide the necessary documentation to show there is likely infringement;"[63] and "turning a blind eye" by actively taking steps to avoid gaining knowledge of the infringement satisfies the knowledge requirement.[64]

In *Arista Records LLC v. Usenet.com, Inc.*, the United States District Court for the Southern District of New York found that an online newsgroup was explicitly put on notice of its users' infringement when the plaintiff record label sent multiple cease-and-desist letters to the defendant, and when users admitted to copyright infringement in their communications with the defendant's technical support staff.[65] In another case, *In re Aimster Copyright Litig.*, the Seventh Circuit held that a defendant file sharing service had knowledge of its users' infringing activity when the defendant turned a blind eye toward the infringement by encrypting all transferred files so that it would be impossible to know which ones were infringing.[66]

---

third-party standing in free speech case because of potential chilling effect of law on others).

60. Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 149 (S.D.N.Y. 2009).

61. *Id.* at 154.

62. *Id.*

63. A&M Records v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001).

64. *Arista*, 633 F. Supp. 2d at 154.

65. *Id.* at 139, 155.

66. In re Aimster Copyright Litig., 252 F. Supp. 2d 634, 651 (N.D. Ill. 2002), *aff'd*, 334

Similar to *Usenet*, a copyright holder can put a privacy service on notice of its customer's infringements by sending notices of infringement to the privacy service's WHOIS address and other addresses listed on the privacy service's website.[67] Specific links to infringing content and screenshots from the infringing website should be attached to the letter to create the strongest possible evidence of infringement. Such documentation should be strong enough to "show there is likely infringement" and preclude a privacy service from arguing that it was not alerted to the infringement due to weak or insufficient evidence.[68]

The privacy service would likely argue that it does not read e-mails sent to the address published in the WHOIS database; rather, it merely forwards e-mails to its customers,[69] and thus it cannot have knowledge of the infringement. However, privacy services are in fact the registrants of the domains they register on behalf of others;[70] domain owners are expected to keep a working e-mail address under ICANN rules;[71] many privacy services claim to comply with ICANN rules in their TOS agreements;[72] and at least one privacy service claims to provide "world-class" responsiveness to inquiries, complete with "24 by 7 telephone support . . . and a responsive staff eager to answer your questions."[73] Consistent failure to respond to infringement notices or affirmatively taking a "neutral"[74] position under such circumstances may be viewed by a court as turning a blind eye to infringement[75]—particularly if the privacy service responds to non-infringement-related inquiries or provides technical support for its customers. Like the encryption in *Aimster*, a privacy service does not insulate itself from knowledge of the infringement by instituting a policy of evading or forwarding all complaints from copyright holders.[76] Accordingly, strong evi-

---

F.3d 643, 650 (7th Cir. 2003) [hereinafter *In re Aimster I*].

67. Domains By Proxy, http://www.domainsbyproxy.com (last visited Nov. 7, 2010) [hereinafter Domains By Proxy Homepage].

68. *Napster*, 239 F.3d at 1021 (quoting *Religious Tech. Ctr.*, 907 F. Supp. at 1374).

69. Domains By Proxy Homepage, *supra* note 67.

70. *See* Domains By Proxy TOS, *supra* note 33; *see also* RAA, *supra* note 24, § 3.7.7.3.

71. RAA, *supra* note 24, §§ 3.7.7.1, 3.7.7.2.

72. *See, e.g.*, Domains By Proxy TOS, *supra* note 33, § 4.

73. *See* About Domains By Proxy, *supra* note 31.

74. *See Solid Host*, 652 F. Supp. 2d at 1098 (quoting a defendant privacy service that stated it would "remain neutral" in a dispute between an infringer customer and an aggrieved trademark holder); *see also* Domains by Proxy FAQ's, *supra* note 39.

75. In re Aimster Copyright Litig., 334 F.3d 643, 650 (7th Cir. 2003) [hereinafter *In re Aimster II*].

76. *Id.* at 650–51 ("Our point is only that a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used.").

dence of infringement delivered to all of the privacy service's advertised addresses should be sufficient to establish at least constructive knowledge of infringement.

C. Material Contribution

The third element of contributory copyright infringement requires "material contribution" to the primary infringement.[77] Material contribution is established when the secondary infringer provides the "site and facilities" for the direct infringement.[78] The most hotly contested issue in a hypothetical suit would be whether a privacy service provides the "site and facilities" for its customer's infringements by providing domain registration service, an Internet address, technical support, and anonymity protection.

In *Fonovisa, Inc. v. Cherry Auction, Inc.*, the Ninth Circuit held that a swap meet owner provided the "site and facilities" for copyright infringement by providing "space, utilities, parking, advertising, plumbing, and customers" for merchants who sold counterfeit recordings on the premises.[79] The court reasoned that "it would be difficult for the infringing [sales] to take place in the massive quantities alleged without the support services provided by the swap meet."[80]

In *Solid Host, NL v. Namecheap, Inc.*, the United States District Court for the Central District of California extended the *Fonovisa* "swap meet" reasoning to the online world.[81] In denying a privacy service's motion to dismiss a trademark holder's contributory trademark infringement claim, the court stated that the privacy service, which acted as the registrant for the domain name used by a "Doe" cybersquatter to commit the underlying offense,[82] had the requisite "direct control and monitoring of the instrumen-

77. *Gershwin*, 443 F.2d at 1162.

78. *Fonovisa*, 76 F.3d at 264.

79. *Id.* at 259, 260, 264.

80. *Id.* at 259, 264.

81. *Solid Host*, 652 F. Supp. 2d at 1115.

82. Cybersquatting in violation of the Anticybersquatting Consumer Protection Act typically involves "[r]egistering a famous trademark as a domain name and then offering it for sale to the trademark owner . . . ." *See Solid Host*, 652 F. Supp. 2d at 1102 (citing Ford Motor Co. v. Catalanotte, 342 F.3d 543, 549 (6th Cir. 2003)); *see also* Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(a). In this atypical case, after the cybersquatter "hack[ed]" into the registrar's system, transferred plaintiff's domain to his or her own account, and transferred the stolen domain to the defendant privacy service, the privacy service licensed control of the domain back to the alleged hacker, who then attempted to ransom the domain name back to the plaintiff. *Solid Host*, 652 F. Supp. 2d at 1102. The court viewed the privacy service as the registrant for the do-

tality" used for infringement[83] to be held liable for contributory trademark infringement.[84] The court reasoned that, similar to a swap meet owner, the privacy service provided the "[I]nternet real estate" utilized by the cybersquatter to hijack the plaintiff's domain name.[85] The court also stated that the "anonymity service [provided] was central to [the] cybersquatting scheme" because the illegal activity would have ceased if the privacy service had simply returned the domain name to the plaintiff.[86]

Like the utilities, parking, and other support services in *Fonovisa*,[87] it would be very difficult to commit website-based copyright infringement without the necessary domain address and privacy-cloaking features that facilitate infringement with impunity. Infringers who use their own domain names as they appear in the WHOIS database can easily be discovered and prosecuted, and such registrations can be terminated by the registrar pursuant to ICANN rules.[88] Because the infringement would be more difficult to commit or even cease completely without provision of the Internet address and the insurance afforded by anonymity, privacy services provide the "site and facilities" for infringement to occur. Although *Solid Host* was a trademark case,[89] the licensing scheme deemed "central" to the infringement scheme in that case[90] is no less central to the copyright infringement at issue here. Just as the illegal activity in *Solid Host*[91] would have ceased upon termination of the privacy protection,[92] infringing website owners would cease their illegal activities if they were exposed to liability upon removal of the anonymity protection.

In response to the copyright holder's argument, a defendant privacy service would: (1) challenge the real estate-Internet address analogy; (2) object to the application of a trademark case in the copyright context; (3) argue that "anonymity" should be extricated from the domain licensing scheme and analyzed as a First Amendment issue; and (4) challenge the causal relationship between providing anonymity and the commission or facilitation of copyright infringement. Each of these counterarguments will

---

main. *Id.* at 1115.

83. *Solid Host*, 652 F. Supp. 2d at 1112 (citing Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 984 (9th Cir. 1999)).

84. *Id.* at 1116.

85. *Id.* at 1115.

86. *Id.* at 1115.

87. *Fonovisa*, 76 F.3d at 264.

88. RAA, *supra* note 24, § 3.7.7.11.

89. *Solid Host*, 652 F. Supp. 2d at 1092.

90. *Id.* at 1115.

91. *Id.* at 1092.

92. *Id.* at 1115.

be examined in turn.

1. The Analogy Between Real Estate and Domain Names

There is some debate over whether infringement cases that arose in the brick-and-mortar context should apply to the Internet.[93] A defendant privacy service would likely object to a comparison of the *Fonovisa* flea market to an Internet address. In *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, the Ninth Circuit held that a defendant credit card company's provision of a payment transaction system for purchases of infringing content over a website did not amount to a material contribution, because the infringing purchases could occur even without the payment transaction system.[94] In reaching its decision, the court rejected the plaintiff's application of the *Fonovisa* case and stated that brick-and-mortar infringement cases should not be applied to the online world.[95]

However, some judges are more willing to accept the real estate-intellectual property connection. The *Solid Host* court comfortably drew an analogy between landowners and domain owners by accepting the flea market analogy and describing the defendant privacy service as a "cyber-landlord of Internet real-estate."[96] The court in *A & M Records, Inc. v. Napster, Inc.* relied on the flea market analogy when it held that "site and facilities" encompasses file storage computers, which are arguably less analogous to real estate than domain names.[97] While computer servers are mobile, domain names, like real estate, derive their value and utility from their unique locations in space.[98] Finally, the *Perfect 10* court explicitly stated that providing a "website" would count as a "site" under the material contribution test.[99] Arguably, privacy services that license domain

93. *See Perfect 10*, 494 F.3d at 798 n.9 ("We similarly take little comfort in the dissent's resurrection of the 'dance-hall-owner/absentee-landlord' cases as a source of any principled distinction in this area. Those tests were developed for a brick-and-mortar world, and . . . they do not lend themselves well to application in an electronic commerce context.").

94. *Id.* at 797–98.

95. *Perfect 10*, 494 F.3d at 798 n.9 ("We similarly take little comfort in the dissent's resurrection of the 'dance-hall-owner/absentee-landlord' cases as a source of any principled distinction in this area. Those tests were developed for a brick-and-mortar world, and . . . they do not lend themselves well to application in an electronic commerce context.").

96. *Solid Host*, 652 F. Supp. 2d at 1115.

97. *Napster*, 239 F.3d at 1022.

98. *See 5 Ways Domain Names Are Better Than Real Estate*, DOMAINNAMEWIRE.COM, Mar. 3, 2008, http://domainnamewire.com/2008/03/03/5-ways-domain-names-are-better-than-real-estate (comparing the value of real estate and online domain names).

99. *Perfect 10*, 494 F.3d at 799 ("The *websites* are the 'site' of the infringement, not De-

names—an essential component of a website—provide their customers with the websites used for infringement.[100] A judge with a fairly sophisticated understanding of the Internet should accept the proposition that privacy services that knowingly lease Internet domains for illegal use contribute to infringement in the same way as landlords or flea market owners who knowingly lease real property for illegal use.

2. Copyright and Trademark Share Similar Principles of Secondary Liability

A defendant privacy service would object to the application of *Solid Host* in the copyright context. However, while the standards for trademark and copyright infringement are fundamentally different,[101] courts have recognized that copyright and trademark share similar principles of secondary liability.[102]

Contributory infringement "originates in tort law and stems from the notion that one who directly contributes to another's infringement should be held accountable."[103] To illustrate, the *Fonovisa* flea market owner was also found liable for contributory trademark infringement for knowingly supplying the necessary marketplace for the sale of infringing products.[104] This is hardly different from the court's rationale for its copyright infringement holding,[105] and, more importantly, the flea market owner's actions satisfied both standards of contributory liability.[106] If a privacy service was found liable for contributory trademark infringement in *Solid Host*,[107] then a privacy service engaging in identical acts of contribution to copyright infringement should also be found liable under similar copyright and tort law principles of secondary liability. Accordingly, privacy services should be held accountable for their contributory acts in either infringement context.

---

fendants' payment networks.").

100. *See* Posting of John Moore to SonicBlog, http://www.sonicweblog.com/pebble/main/2007/08/21/1187728020000.html (Aug. 21, 2007, 13:27 PST) (identifying the domain name, hosting, and website files as the three essential components of a website).

101. *Sony*, 464 U.S. at 439 n.19.

102. *Fonovisa*, 76 F.3d at 259, 261.

103. *Id.* at 259, 264.

104. *Id.* at 259, 265.

105. *Id.* at 261, 264 ("[I]t would be difficult for the infringing activity to take place in the massive quantities alleged without the support services provided by the swap meet.").

106. *Id.* at 259.

107. *Solid Host*, 652 F. Supp. 2d at 1092.

3. Anonymity Is Not an Independent Contribution to Infringement

The "site and facilities" question may hinge on whether providing a domain name and anonymity are regarded by the court as separate contributions to infringement. Answering this question requires a technical understanding of how "privacy" is administered. The registrar is the entity that maintains the WHOIS database and publishes registrants' information therein.[108] The privacy service's act of registering a domain on behalf of its customer automatically triggers the input of the privacy service's information into the WHOIS database in place of the customer's, which produces the bait-and-switch described as "anonymity." [109] No anonymity is provided independently from the process of registering a domain on behalf of a third party.[110] Thus, "privacy service" is a composite service involving domain registration, domain licensing, and the resulting anonymity protection—none of which can be isolated and analyzed as separate, volitional acts of contribution. A privacy service, however, would ask the court to scrutinize anonymity as a separate contribution that, if considered alone, raises a causation issue and implicates the customer's First Amendment right to speak anonymously online.[111]

A court is not likely to concentrate solely on "anonymity" as an independent contribution to infringement. In *Fonovisa*, the court rejected the defendant's argument that the "leasing of space" should be scrutinized in isolation, and instead considered the leasing of space in the broader context of providing "the environment and the market for counterfeit recording sales to thrive."[112] The court considered the combined effect of providing the "space, utilities, parking, advertising, plumbing, and customers"[113] without scrutinizing the causal relationship between providing toilets and the infringement. Similarly, the insurance against prosecution afforded by anonymity should be viewed in the larger context of providing an online safe haven for known infringers which also offers domain registration services, as well as technical support.[114] The overall "environment" created by

108. RAA, *supra* note 24, § 3.3.

109. *See* Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 982 (9th Cir. 1999) (explaining that the domain registration process is usually electronic and without human intervention).

110. *See Solid Host*, 652 F. Supp. 2d at 1096.

111. *See* Solers, Inc. v. Doe, 977 A.2d 941, 950 (D.C. 2009) (observing that anonymous Internet speech is protected by the First Amendment).

112. Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996)..

113. *Id.*

114. *See* About Domains By Proxy, *supra* note 31.

the privacy service's contributions is relevant under *Fonovisa*,[115] and given that the anonymity is technically inextricable from domain registration, a court is unlikely to scrutinize anonymity in isolation.[116]

4. Causation

Causation is not a required element of contributory copyright infringement,[117] but at least one court has read an element of "but for" causation into the material contribution analysis. In *Perfect 10*, a credit card company was not liable for contributory copyright infringement when it provided an online payment transaction system for an infringing website because the card company "[had] no direct connection to [the] infringement."[118] The court stated that the card company did not cause the infringement because the infringement could continue even without the payment system,[119] and because "[a]ny conception of 'site and facilities' that encompasses [credit card companies] would also include a number of peripherally-involved third parties, such as . . . utility companies that provide electricity to the Internet."[120] Similarly, a defendant privacy service would argue that providing anonymity is a "peripheral" contribution akin to providing electricity, that the infringement would continue even if the privacy protection were lifted, and that privacy protection cannot therefore be the cause of the infringement.

The privacy service is not a "peripheral" contributor to the infringement because it contributes the domain name—a major component of a "website," which the *Perfect 10* court stated would qualify as a material contribution.[121] The very nature of the Internet and the website format is in the domain name system itself: Internet addresses are the gateways to the server computers that comprise the Internet,[122] and providing such access

---

115. *See Fonovisa*, 76 F.3d at 264.

116. *See infra* § II(D) (arguing that a privacy service cannot invoke the First Amendment right to speak anonymously as a defense to copyright infringement).

117. *See Fonovisa*, 76 F.3d at 264 ("[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer." (quoting *Gershwin*, 443 F.2d at 1162)). The "or" suggests that causation is not a strict requirement of contributory copyright infringement.

118. Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 796 (9th Cir. 2007).

119. *Id.* at 798.

120. *Id.* at 800.

121. *See id.* at 799.

122. *See* Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 981-82 (9th Cir. 1999) ("When [a person] seeks to maintain an Internet web site, that [person] must reserve . . . an Internet Protocol ('IP') Address . . . . When an Internet user accesses the [person's] web site, the user enters the domain-name combination that corresponds to the IP Address and is routed to the

points should be encompassed in the Ninth Circuit's conception of a "website" as a "site and facility" for online infringement.[123] The added effect of anonymity only magnifies the privacy service's assisting role in the infringement, as it would be near impossible to operate an infringing website for long without the aid of an anonymous domain name. As the district court duly noted in *Solid Host*, "[i]f [the privacy service] had returned the domain name to [the plaintiff], Doe's illegal activity would have ceased."[124] Accordingly, privacy services do play a central causal role in their customers' infringing activities.

D. Anonymous Infringement is Not a Constitutionally Protected Right

Apart from objecting to discovery requests on First Amendment grounds, the privacy service would argue that imposing liability for providing anonymity service would violate the First Amendment rights of its customers to speak anonymously,[125] as asserted on their behalf by the privacy service.[126] While privacy services might be inclined to frame any legal claim against them as an attack on anonymity itself, courts have consistently recognized that "[t]hose who suffer damages as a result of tortious or other actionable communications on the Internet should be able to seek appropriate redress by preventing the wrongdoers from hiding behind an illusory shield of purported First Amendment rights."[127] The District of Columbia Court of Appeals has stated that the law must strike a balance "between the well-established First Amendment right to speak anonymously and the right of the plaintiff to protect its proprietary interests . . . through the assertion of recognizable claims based on the actionable con-

---

host computer.").

123. *See Perfect 10*, 494 F.3d at 799–800.

124. *Solid Host*, 652 F. Supp. 2d at 1115.

125. *See Solers*, 977 A.2d at 950 (observing that anonymous Internet speech is protected by the First Amendment).

126. The privacy service would likely have standing to assert such a right on behalf of its customers. *NAACP*, 357 U.S. at 459; Virginia v. Am. Booksellers Ass'n, 484 U.S. 383, 392–93 (1988) (allowing third-party standing in free speech case because of the potential chilling effect of a law on others).

127. *Solers*, 977 A.2d at 951 n.7 (quoting *In re* Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26, 35 (Va. Cir. Ct. 2000)); *see also Columbia*, 185 F.R.D. at 578 (stating that "[w]ith the rise of the Internet has come the ability to commit certain tortious acts, such as defamation, copyright infringement, and trademark infringement, entirely on-line . . . . People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law.").

duct of the anonymous, fictitiously-named defendant."[128] More specifically, courts have consistently recognized that the First Amendment does not protect copyright infringement.[129]

Here, the manner in which the privacy service achieves a customer's disappearance from the WHOIS database—by ceding control of the domain name to a known infringer while retaining ownership—amounts to an act of contributory copyright infringement in itself for all of the foregoing reasons.[130] Assuming the elements of contributory copyright infringement are met, the First Amendment does not bar the imposition of infringement liability on privacy services,[131] even if the licensing scheme produces an incidental "anonymity" effect on its users.

Accordingly, privacy services should not receive First Amendment protection in the limited situation in which they license domain names to customers who they know are engaged in infringement. Anonymous speech is a fundamental right,[132] but a court should not tolerate the abuse of anonymity to further the commission of infringement.

E. Sony-Betamax Does Not Protect Privacy Services

In *Sony Corp. of America v. Universal City Studios, Inc.*, the Supreme Court held that a maker of a video recording device was not liable for contributory copyright infringement when it sold the device to consumers who used the device to make copies of television broadcasts of copyrighted material.[133] The court borrowed a patent statute providing that "the sale of a 'staple article or commodity of commerce suitable for substantial noninfringing use' is not contributory infringement,"[134] and, in recognizing the similarities between patent and copyright law,[135] applied the doctrine in the

---

128. *Solers*, 977 A.2d at 951.

129. *See* Sony Music Entm't, Inc. v. Does 1–40, 326 F. Supp. 2d 556, 562–63 (S.D.N.Y. 2004) ("The First Amendment . . . does not protect copyright infringement . . . ."); *see also* Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 555–60, 569 (1985) (holding that a copyright violation which did not qualify as a "fair use" of the copyrighted material was not protected speech under the First Amendment). This article assumes that the copyright holder has a strong infringement claim against the primary infringer, and that "fair use" does not apply.

130. *See supra* § II.A–C.

131. *See Sony Music Entm't*, 326 F. Supp. 2d at 562–63 ("The First Amendment . . . does not protect copyright infringement . . . ."); *see also Harper & Row*, 471 U.S. at 555–60, 569 (holding that a copyright violation which did not qualify as a "fair use" of the copyrighted material was not protected speech under the First Amendment).

132. *Solers*, 977 A.2d at 950.

133. *Sony*, 464 U.S. at 442.

134. *Id.* at 440 (quoting 35 U.S.C. § 271(c)).

135. *Sony*, 464 U.S. at 439, 442 ("We recognize there are substantial differences between

copyright context. Staple articles of commerce include typewriters, recorders, cameras, and photocopying machines,[136] all of which are capable of both infringing and legitimate uses;[137] and the court reasoned that imposing liability for selling copying equipment would disrupt consumers' rights to freely engage in areas of commerce substantially unrelated to the copyright sought to be protected.[138]

Innovations in copying technology have inspired a revival of the "staple article of commerce" defense in Internet cases.[139] In *Arista Records LLC v. Usenet.com, Inc.*, the court rejected a defendant's "staple article" defense to contributory copyright infringement when the defendant operated an online newsgroup in which users posted and downloaded infringing music files,[140] and the defendant assisted users by providing live technical support.[141] The court stated that a critical part of the "staple article" defense is that the product maker maintains no ongoing relationship with the end-user after the point of sale.[142] Far from doing so, and unlike manufacturers of video recorders, the defendant in *Usenet* maintained an ongoing relationship with users by providing technical support for their illegal downloads, among other communications.[143]

Domain privacy services are clearly capable of non-infringing uses. Privacy services arguably have some legitimate social value, as they allow Internet users to prevent spammers and data harvesters from gathering personal information from the WHOIS database.[144] However, unlike the sale of a video recorder, there is no single "point of sale" after which a privacy service severs its relationship with end-users.[145] To the contrary, privacy services retain ownership of their customers' domains,[146] provide twenty-

---

the patent and copyright laws. But in both areas the contributory infringement doctrine is grounded on the recognition that adequate protection of a monopoly may require the courts to look beyond actual duplication of a device or publication to the products or activities that make such duplication possible.").

136. *Id.* at 426.

137. *Id.*

138. *Id.* at 442.

139. Wikipedia, Sony Corp. of Am. v. Universal City Studios, Inc., http://en.wikipedia.org/wiki/Sony_Corp._of_America_v._Universal_City_Studios,_Inc. (last visited Sept. 14, 2010) (referring to various cases in which the Sony-Betamax defense was raised).

140. *Arista*, 633 F. Supp. 2d at 133, 156.

141. *Id.* at 133.

142. *Id.* at 156.

143. *Id.* at 133, 156.

144. *See* Domains By Proxy Homepage, *supra* note 67.

145. *See* Domains By Proxy TOS, *supra* note 33.

146. *See id.*

four hour technical support,[147] share e-mail addresses with their customers,[148] refuse to disclose their customers' identities without express permission,[149] and assume the online identities of their customers by replacing them in the WHOIS database.[150] This conduct demonstrates the type of ongoing relationship found in *Usenet*.[151] Accordingly, privacy services are not sufficiently insulated from infringement to raise a complete defense under *Sony-Betamax*.[152]

F. Privacy Services Should Not Qualify for DMCA Safe Harbor Protection

A defendant privacy service would likely attempt to raise a DMCA Section 512(a) "safe harbor" defense to contributory copyright infringement.[153] DMCA Section 512(a) provides immunity to contributory infringement claims against "service provider[s]" that offer "routing" and "transmission" functions.[154] In *RIAA v. Verizon*, the Ninth Circuit stated that the Section 512(a) safe harbor applies to Internet service providers performing functions such as providing Internet access and "transmitting e-mails, instant messages, or files sent by an [I]nternet user from his computer to that of another [I]nternet user."[155] In another case, *In re Aimster Copyright Litig.*, the United States District Court for the Northern District of Illinois held that a defendant peer-to-peer file transfer service was not eligible for Section 512(a) immunity because the service did not merely enable file transfer between users, but also offered file search capabilities, automatic resumption of interrupted downloads, one-click downloads of the most popular titles, and editorial comment on popular titles.[156] The court reasoned that the defendant did more than provide a "mere conduit" for information passing through the system.[157]

Assuming a domain privacy service falls under the broadly defined "service provider" designation,[158] a privacy service would need to show

147. *See* About Domains By Proxy, *supra* note 31.

148. *See* How Private Registrations Work, *supra* note 3.

149. Domains By Proxy TOS, *supra* note 33, § 1.

150. *Id.*

151. *Arista*, 633 F. Supp. 2d at 156.

152. *Sony*, 464 U.S. 417.

153. *See* 17 U.S.C. § 512(a) (2006).

154. 17 U.S.C. § 512(a).

155. Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1237 (D.C. Cir. 2003).

156. *In re Aimster I*, *supra* note 66, at 660.

157. *Id.* at 660.

158. *Id.* at 658.

that it performs "routing" or "transmission" functions,[159] yet provides nothing more than a "mere conduit" for information passing between Internet users.[160] First, privacy services offer none of the file transfer or Internet access functions offered by the *Verizon* court as examples of routing or transmission functions;[161] and unlike *Aimster*,[162] no infringing material passes through the privacy service's computer systems. Licensing one's domain name for another's use merely alters the registration information in the WHOIS database,[163] which involves no routing, transmission, or storage of users' files.[164] Moreover, simply offering an e-mail forwarding service should not allow a privacy service to claim that it offers a "transmission" function and escape liability, because the central function of the privacy service is to provide anonymity—not e-mail service. Contributory infringement would be meaningless if every facilitator of infringement could qualify for Section 512(a) immunity simply by adding e-mail forwarding to its list of offered services.

A registrar is an example of a service provider that might qualify for DMCA Section 512(a) immunity to contributory copyright infringement. Registrars such as GoDaddy.com[165] arguably provide nothing more than a routing function by connecting domain names to IP addresses,[166] a process which forms the basis of the Internet.[167] While many privacy services are affiliated with registrars,[168] they are not registrars in any sense.[169] Privacy services are themselves the registrants and owners of the domains they license to their customers,[170] and Section 512(a) would be meaningless if it immunized all domain registrants from infringement liability. Privacy services are more akin to dealers of domain names—indeed "cyberlandlord[s]"—than passive providers of an Internet routing function.[171] The *Solid Host* court adopted this position when it compared a defendant

159. 17 U.S.C. § 512(a).

160. *In re Aimster I*, *supra* note 66, at 660.

161. *Verizon*, 351 F.3d at 1237.

162. *In re Aimster I*, *supra* note 66, at 660.

163. *See* About Domains By Proxy, *supra* note 31.

164. Domains By Proxy TOS, *supra* note 33.

165. GoDaddy.com, *supra* note 23.

166. *See* Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 982 (9th Cir. 1999) (describing how registrars provide Internet connectivity).

167. *Id.*

168. *See* About Domains By Proxy, *supra* note 31.

169. *See id.*

170. RAA, *supra* note 24, § 3.7.7.3; *see also* Domains By Proxy TOS, *supra* note 33.

171. Solid Host, NL v. Namecheap, Inc., 652 F. Supp. 2d 1092, 1114 (C.D. Cal. 2009).

privacy service to a property owner instead of a registrar: the "[defendant's] position is closer to that of a flea market operator . . . than . . . a registrar."[172] Privacy services do not connect their customers directly to the Internet; rather, they buy pieces of the Internet and lease them to their customers, not unlike a flea market owner.[173] There is no DMCA Section 512(a) protection for that activity when it is knowingly done to assist an infringer.[174]

In sum, privacy services do not offer any "routing" or "transmission" functions because no infringing material passes through their computer systems, and domain licensing does not equate to merely providing Internet access. Domain licensing is outside the purview of DMCA Section 512(a) protection, and the safe harbor defense should fail.

III. BEFORE LITIGATION, A COPYRIGHT HOLDER SHOULD SEND THE PRIVACY SERVICE A NOTICE OF INFRINGEMENT AND DEMAND THE INFRINGER'S CONTACT INFORMATION

A copyright holder should pursue any and all avenues of obtaining an infringer's identity before considering litigation. The first step is to send the privacy service a notice of infringement and demand for the infringer's contact information. The letter serves two purposes: to put the privacy service on notice of infringement in anticipation of suit, and to give the privacy service a chance to avoid litigation by revealing the infringer. Support for this demand letter is found in (1) ICANN's policies, (2) some of the privacy services' own TOS agreements, and (3) case law as described in Part II of this article.

A. Failure to Respond to a Demand Letter is a Violation of ICANN Rules

A privacy service's failure to respond to a written demand letter is a violation of ICANN rules, and this should be made clear in any demand letter.[175] All ICANN-accredited registrars must abide by ICANN's Registrar Accreditation Agreement (RAA) or risk losing accreditation.[176] The RAA requires all registrars to enter an agreement with registrants including the following three provisions: (1) although registrations on behalf of third party licensees are permitted under the RAA, the Registered Name Holder

172. *Id.* at 1115.
173. *Id.* at 1114.
174. 17 U.S.C. § 512(a).
175. RAA, *supra* note 24, § 3.11.5.
176. RAA, *supra* note 24, § 5.3.

must provide "information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name";[177] (2) the Registered Name Holder must "accept liability for harm caused by wrongful use of the Registered Name, unless it promptly discloses . . . the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm";[178] and (3) the Registered Name Holder represents that, to the best of the name holder's knowledge, the Registered Name does not directly or indirectly infringe the "legal rights of any third party".[179]

Privacy services that provide their own contact information for the WHOIS database but fail to respond to copyright infringement complaints, or merely forward the complaints to their nonresponsive customers, do not provide any information sufficient to resolve infringement problems occurring in connection with the domain. Thus, they are likely to be in violation of RAA Section 3.7.7.3.[180] Next, copyright infringement should constitute "harm caused by wrongful use of the Registered Name,"[181] because the infringement could not occur without the domain functioning as a locus for the infringing activity. Privacy services that own and license such domains while refusing to either reveal licensee infringers' identities or accept liability themselves are in breach of RAA Section 3.7.7.3.[182] Finally, privacy services that refuse to address infringement after receiving the first complaint from a copyright holder violate RAA Section 3.7.7.9 by knowingly allowing their domain registrations to continue to be used for copyright infringement.[183]

Unfortunately for copyright holders, the RAA specifically excludes third party beneficiaries from bringing claims for breach of the RAA,[184] which precludes copyright holders from enforcing the RAA against Registered Name Holders. Nevertheless, demand letters should remind privacy services that if they do not reveal their infringing customers' contacts, ICANN may hold them responsible for their customers' acts of infringement under the RAA,[185] and registrars may enforce the RAA against pri-

177. RAA, *supra* note 24, § 3.7.7.3.
178. *Id*.
179. RAA, *supra* note 24, § 3.7.7.9.
180. *See* RAA, *supra* note 24, § 3.7.7.3.
181. *Id.*
182. *Id.*
183. *See* RAA, *supra* note 24, § 3.7.7.9.
184. RAA, *supra* note 24, § 5.10.
185. *See* RAA, *supra* note 24, § 3.7.7.3.

vacy services by suspending, terminating, or transferring their registrations.[186]

B. Failure to Reveal an Infringer's Identity is a Violation of Most Privacy Services' TOS Agreements

Most privacy services' Terms of Service (TOS) agreements are drafted in compliance with ICANN rules,[187] so a violation of ICANN rules is likely to be a violation of the privacy service's own TOS agreement as well. For example, WhoisGuard's TOS states that it will make available its customers' registration information "to third parties as ICANN and applicable laws may require or permit,"[188] and Domains by Proxy's TOS reserves the absolute right and power to reveal personal information in order "to comply with ICANN rules, policies or procedures."[189] A privacy service's violation of its own policy might be viewed by a court as an endorsement of its customers' infringing acts, despite the privacy service's declarations of intended legal compliance in its TOS. Evidence of a violation of the TOS could be used against the privacy service in a lawsuit. A demand letter to a privacy service should specifically include such a warning.

C. Privacy Services That Refuse to Reveal Their Infringing Customers Should be Warned About Exposure to Liability

Privacy services may choose not to respond to requests for contact information based solely on alleged violations of the ICANN and TOS agreements. However, a strong demand letter should mention that legal liability may exist for privacy services that refuse to reveal infringers under recent case law.[190] The demand letter should mention *Solid Host*,[191] and it should caution broadly that joint liability exists for intellectual property infringement.[192] This should sufficiently pressure the privacy service to release the infringers' contact information, but there are potential risks. One

---

186. RAA, *supra* note 24, § 3.7.7.11.

187. *See, e.g.*, Domains By Proxy TOS, *supra* note 33, § 4; WhoisGuard TOS, *supra* note 34, § 8.

188. WhoisGuard TOS, *supra* note 34, § 8.

189. Domains By Proxy TOS, *supra* note 33, § 4.

190. *See, e.g.*, Solid Host, NL v. Namecheap, Inc., 652 F. Supp. 2d 1092, 1092 (C.D. Cal. 2009).

191. *Id.*

192. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996) ("[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer." (quoting *Gershwin*, 443 F.2d at 1162)).

significant risk is that such a letter-writing campaign may encourage privacy services to move offshore out of fear of liability to U.S. copyright holders, which could create jurisdictional obstacles for copyright holders seeking redress for infringement.

IV. CONCLUSION

A new demand letter to privacy services should be drafted stating that (1) privacy services violate the Internet Corporation for Assigned Names and Numbers' (ICANN) Registrar Accreditation Agreement (RAA) Sections 3.7.7.3 and 3.7.7.9 by refusing to divulge infringing customers' information or accept legal liability for the infringement;[193] (2) privacy services may be in violation of their own Terms of Service (TOS) agreements by refusing to reveal infringers, and such a violation can be used against them in a lawsuit;[194] and (3) privacy services should be found liable for intellectual property infringement under recent case law.[195]

If a demand letter yields no response, a copyright holder should prevail against a privacy service on a contributory copyright infringement claim.[196] A court may be reluctant to accept the necessary analogies between copyright and trademark law[197] and between real estate and intellectual property.[198] Furthermore, the privacy service may challenge the causation[199] and raise First Amendment objections.[200] A privacy service is not likely to raise a successful *Sony-Betamax,*[201] defense because privacy serv-

193. *See* RAA, *supra* note 24, §§ 3.7.7.3, 3.7.7.9.

194. *See* Domains By Proxy TOS, *supra* note 33, §4.

195. *See* Fonovisa, Inc. v. Cherry Auction, Inc*.,* 76 F.3d 259, 264 (9th Cir. 1996) ("[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer." (quoting *Gershwin*, 443 F.2d at 1162)); Solid Host, NL v. Namecheap, Inc., 652 F. Supp. 2d 1092, 1092 (C.D. Cal. 2009).

196. *See supra* Part II.

197. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 439 n.19 (1984) (rejecting "the proposition that a . . . kinship exists between copyright law and trademark law . . . ."). *See also* United Drug Co. v. Theodore Rectanus Co., 248 U.S. 90, 97 (1918) (stating that a trademark right "has little or no analogy" to a copyright or patent (citing Canal Co. v. Clark, 80 U.S. 311 (1872))); *supra* Part II.C.2.

198. *See supra* Part II.C.1.

199. *See supra* Part II.C.4.

200. *See supra* Part II.D; *see also* Religious Tech. Ctr. v. Netcom On-Line Commc'n. Servs., Inc., 907 F. Supp. 1361, 1383 (N.D. Cal. 1995) (raising First Amendment concerns about imposing copyright infringement liability when injunction against Internet service provider would chill its users' speech).

201. *Sony*, 464 U.S. at 417.

ices are not sufficiently insulated from their customers to disclaim responsibility for their actions.[202] A privacy service is also unlikely to raise a successful Digital Millennium Copyright Act (DMCA) Section 512(a) safe harbor defense, because domain licensing is not a "routing" or "transmission" function akin to providing Internet access or file transfer services.[203] A successful contributory copyright infringement suit against a privacy service would set a useful precedent and hopefully help ease the enforcement burdens of copyright holders.

V. SAMPLE DEMAND LETTER TO PRIVACY SERVICES

Date
[Copyright Holder]
Sent by: [_____]
[Law Firm Name]
[Law Firm Address]

[Recipient Privacy Service Name/Address]

Re: NOTIFICATION OF ILLEGAL USE OF YOUR REGISTERED DOMAIN AND REQUEST FOR USER CONTACT INFORMATION

This is a notification on behalf of [copyright holder] regarding infringements of [copyright holder's] intellectual property rights occurring at the web domain www._____.com, which is registered in your name. In accordance with ICANN's Registrar Accreditation Agreement (RAA), your terms of service agreement with the licensee operator of www._____.com, and federal law, we request that you immediately provide contact information for the licensee and operator of the aforementioned domain or assume liability for the infringement of [copyright holder's] intellectual property rights.

Pursuant to ICANN RAA Section 3.7.7.3, you are required to provide contact information sufficient for copyright holders to address infringement occurring in connection with your domain in a timely manner or accept liability for such infringement. Further, under RAA Section 3.7.7.9, you

202. *See supra* Part II.E.
203. *See supra* Part II.F.

also represent that your registration will not be used to infringe the copyright of any third party.

In addition, as you may already be aware, your [Terms of Service Agreement] states your intention to comply with ICANN policies and the law. [This section must be tailored for each privacy service as their terms of service vary]. Specifically, [common language in terms of service agreements states that the service will identify infringers who break ICANN rules and/or the law].

Furthermore, as you likely are aware, recent federal case law holds that privacy services may be liable for operators' underlying intellectual property infringement.[204] Should you refuse to identify the aforementioned infringer, we caution that you may be exposed to liability for your domain licensees' usage of your registered name for purposes of infringement.

Accordingly, we request that you provide information sufficient for [copyright holder] to identify the operator of *www.*_____*.com* so that we may contact them directly regarding the infringement. Any refusal to comply with this request may expose you to liability for the underlying infringement, and in addition, your registrar may be required to terminate your registration under RAA Section 3.7.7.11.

The following links and screenshots demonstrate unauthorized use of [copyright holder's] content at *www.*_____*.com*, which is registered in your name:

[Links]

[Screenshots]

In addition to providing a working contact for the licensee operator of your domain, we ask that you preserve all evidence of infringement, including any correspondence with the operator, in anticipation of [copyright holder] serving a subpoena to obtain this information through legal process.

---

204. *See Solid Host*, 652 F. Supp. 2d at 1092, 1105–06; *see also* Transamerica Corp. v. Moniker Online Servs., 672 F. Supp. 2d 1353, 1363–64 (S.D. Fla. 2009) (denying domain privacy service's motion to dismiss plaintiff's contributory cybersquatting claim).

Sincerely,

[Counsel]
[Firm]

Paulo André de Almeida[205]

205 J.D. Loyola Law School, Los Angeles 2011; B.A., University of Southern California. Special thanks to Professor Christopher Hawthorne for his helpful comments on this project. Thank you to Camila Reartes for encouraging me to submit this article for publication, and many thanks to my family and friends for their support and helpful critiques of my work.