Hidden Whois and Infringing Domain Names: Making the Case for Registrar Liability

Ian J. Block
Ian.Block@chicagounbound.edu

Follow this and additional works at: http://chicagounbound.uchicago.edu/uclf

Recommended Citation
Available at: http://chicagounbound.uchicago.edu/uclf/vol2008/iss1/12

This Comment is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in University of Chicago Legal Forum by an authorized administrator of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.
Hidden Whois and Infringing Domain Names: Making the Case for Registrar Liability

Ian J. Block†

INTRODUCTION

When registering domain names for websites, registrants must supply contact information that appears in the Whois database. The Internet Corporation for Assigned Names and Numbers ("ICANN") maintains the Whois database as a means of making information available about website owners (registrants), so that disputes concerning those sites can be resolved quickly.¹ Increasingly, domain name registrars are offering registrants the option to purchase additional services, sold as "hidden Whois"² or "Whois privacy"³ services. When a registrant em-

† BA 2006, Georgetown University; JD Candidate 2009, University of Chicago.
2 Spot Domain LLC Products and Services, <http://www.dominainsite.com/web_enhancement/hidden_whois.php> (last visited May 15, 2007) (explaining Spot Domain’s Hidden Whois service). This explanation, however, is an inaccurate reflection of the information that actually appears as a result in a Whois directory search. Spot Domain claims that “[o]ur Hidden Whois service will hide all registrar whois information for your domain name except for your first, last, and company name”; however, none of the unhidden information appears in Whois directory search results. Accordingly, the actual identity of registrants using this service cannot be ascertained unless released by Spot Domain.
ploys this feature, the registrar's contact information appears in the registration information section of the Whois report for the domain name. As such, the true registrant is an undisclosed principal whose actual information never appears in the Whois database.4 Hidden Whois services were devised initially to help registrants deflect spam that was sent to addresses found in the Whois database,5 but it is believed that such services are increasingly used to shield registrants from litigation arising from their websites. By only being able to find a registrar's information when searching the Whois database, a prospective plaintiff is unable to ascertain the identity of the contested site's registrant, which effectively serves to undermine the purpose, value, and efficacy of the Whois database.

This Comment proposes that courts interpret existing trademark law to find registrar liability when registrars appear as registrants in the Whois database for infringing domain names. The Comment will proffer a legal theory for private trademark enforcement by developing the position that such registrar liability can and should be found under present statutes.

Part I provides historical and technical background information about cybersquatting, as well as the evolution of legislative and judicial efforts to enforce its prevention. This part of the Comment reviews the context of the Anticybersquatting Consumer Protection Act's ("ACPA")6 passage and subsequent application. The ACPA explicitly created a statutory tort barring cybersquatting. The liability rule proposed in Part II of this Comment would operate as a strong reading of the ACPA under its existing framework and intent.

Part II sets out the argument for adopting the proposed liability rule by explaining its statutory justification under the ACPA and applicability under prevailing agency principles. This section details the effects of the proposed rule on ACPA remedies and calls attention to the benefits and efficiencies created by adopting the proposed liability rule. Part II also responds to potential criticisms that might be levied against the proposed rule.

---

4 See Restatement (Third) of Agency § 1.04(2)(b) (2006) (defining a principal as undisclosed if, when an agent and a third party interact, the third party has no notice that the agent is acting for a principal).
Part III concludes that the history and evolution of internet domain name usage, together with Congress' legislative pronouncement against cybersquatting, highlights the need for this Comment's proposed liability rule to prevent cybersquatting. Hidden Whois services promote evasion from private trademark law enforcement, so adopting the liability rule against domain name registrars offering such services will aid in enforcement efforts and cybersquatting prevention.

I. BACKGROUND

The routers that shuffle packets of information across the internet respond to numeric IP addresses that denote the location of internet sites. These addresses take the form of four numbers that are delimited by periods, such as 121.7.106.83. Because humans appreciate alphanumeric mnemonic devices over complicated numerical sequences, IP addresses are set to correspond to more accessible domain names. Therefore, domain names identify websites on the internet for the purposes of user navigation. Users are able to type domain names into internet browsers to access websites on the internet. These domain names, then, are the signifiers that users recognize as the effective addresses of their internet destinations. Companies use trade names, nicknames, abbreviations, or other names recognizable to consumers as internet domain names, since these familiar terms are easily recalled and used by consumers. Users' internet searches often begin with a business's domain name, making the domain name one of the most important business identifiers today.

8 Id.
9 Id ("An IP address looks like 121.7.106.83, where each period separates one of the bytes expressed in decimal notation from 0 to 255. An IP address is hierarchical because as we scan the address from left to right, we obtain more and more specific information about where the host is located in the internet (that is, within which network, in the network of networks). Similarly, when we scan a postal address from top to bottom, we obtain more and more specific information about where the addressee is located."). The Domain Name System ("DNS") converts alphanumeric domain name inputs into machine recognizable IP addresses.
11 Kurose, Computer Networking at 123 (cited in note 7).
12 J. Theodore Smith, Note, "1-800-RIPOFFS.COM": Internet Domain Names are the Telephone Numbers of Cyberspace, 1997 U Ill L Rev 1169, 1169–70 (1997).
13 Gregory R. Jones, What's in a Name? Trademark Infringement in Cyberspace, 68
Domain name registration is overseen by ICANN. Registrants are the parties that come to own individual domain names for use. They pay registrars to register desired and available domain names. Registrars supply ICANN with information, which leads to the activation of the registered domain name. Domain names are distributed on a first come, first served basis; therefore, once a registrant registers a specific domain name it becomes unavailable for registration by others. In their standard capacities, registrars help potential registrants identify available domain names and then register those names with ICANN so that they can be used by registrants.

Aided by an inexpensive registration process and incentivized by the possibility of reaping windfalls from trademark holders, cybersquatting is a significant problem for domain name registration and protecting trademark rights online. In general, cybersquatting is the practice of registering or using a domain name in which others have legitimate interests and then attempting to sell that name either to the trademark owner or to the highest bidder. As the internet has grown in prominence as a medium for commerce and communications, so too has the prevalence of cybersquatting. Various forms of cybersquatting include: 1) registering another's mark as a domain name; 2) registering a misspelling of another's mark as a domain name, commonly referred to as "typosquatting"; 3) registering another's mark as a domain name in top level domains other than .com (for instance, .biz, .cc, .fr, or .tv); 4) registering another's mark as part of a domain name; and 5) registering another individual's name as a domain.

Trademark infringement by cybersquatting presents a fundamental economic and analytical difference from standard trademark infringement. Trademarks in the real world, such as logos, brand names, and other marks, are public goods insofar as infringing use does not prevent the trademark owner from using his mark; however, domain names are private goods because

---


16 Borgman, 8 Tex Intel Prop L J at 266 (cited in note 10).

17 Id.
there can only be one owner of any given unique domain name. For example, whereas any number of firms could physically sell goods under the Acme brand name simultaneously, there can be only one owner and user of the domain name www.acme.com. That domain names are excludable compounds the harms created by cybersquatters.

Cybersquatting creates numerous harms. As the Senate found in its Report on the ACPA, "[t]he practice of cybersquatting harms consumers, electronic commerce, and the goodwill equity of valuable U.S. brand names, upon which consumers increasingly rely to locate the true source of genuine goods and services on the Internet."18

Prior to the 1999 enactment of the ACPA, which explicitly barred cybersquattting, victims sought to enforce their rights in cyberspace under traditional trademark law. In Panavision International v Toeppen,19 plaintiff Panavision owned trademarks for the term Panavision, but was unable to register the internet domain name Panavision.com because defendant Dennis Toeppen previously registered and owned the domain name.20 Panavision's counsel sent a letter to Toeppen pointing out Panavision's ownership of marks and demanding that Toeppen cease to use the mark as a domain name. Toeppen refused, instead offering to sell the domain name to Panavision to "settle the matter."21 When Panavision refused to buy the domain name, Toeppen registered the domain name PanaFlex.com, which corresponded to another of Panavision's trademarks.22 In the absence of federal law explicitly barring cybersquatting at that time, Panavision sued under anti-dilution provisions of state and federal trademark laws.23 Panavision won summary judgment in the district court.24

---

18 S Rep No 106-140 at 5 (cited in note 15).
19 141 F3d 1316 (9th Cir 1998).
20 Id at 1318-20.
21 Id at 1319. As recounted by the Court: "Toeppen responded by mail to Panavision in California, stating he had the right to use the name Panavision.com on the Internet as his domain name. Toeppen stated: 'If your attorney has advised you otherwise, he is trying to screw you. He wants to blaze new trails in the legal frontier at your expense. Why do you want to fund your attorney's purchase of a new boat (or whatever) when you can facilitate the acquisition of 'PanaVision.com' cheaply and simply instead?'
22 Id.
23 Panavision, 141 F3d at 1319 ("Panavision alleged claims for dilution of its trademark under the Federal Trademark Dilution Act of 1995, 15 U.S.C. § 1125(c), and under the California Anti-dilution statute, California Business and Professions Code § 14330.").
On Toeppen's appeal, the Ninth Circuit evaluated the case under a dilution rubric.\textsuperscript{25} At that time, dilution required that: 1) the mark was famous; 2) the defendant was making a commercial use of the mark in commerce; 3) the defendant's use began after the mark became famous; and 4) the defendant's use of the mark diluted the quality of the mark by diminishing the capacity of the mark to identify and distinguish goods and services.\textsuperscript{26} Toeppen challenged the district court's finding that his use of the Panavision mark as his domain name was a commercial use, arguing that merely using a trademark as a domain could not constitute commercial use under existing law.\textsuperscript{27} The court recognized that case law supported Toeppen's argument that the mere registration and use of a domain name was not commercial use,\textsuperscript{28} but the court went on to conclude that Toeppen's use was a commercial use because his cybersquatting and attempts to sell the trademarked domain names to their rightful owners were commercial uses.\textsuperscript{29} Apparently swayed heavily by Toeppen's strong commercial use of Panavision's marks,\textsuperscript{30} the court held that Toeppen's use diluted Panavision's marks. The court noted that the cybersquatting increased search and information costs upon plaintiff's customers by requiring them to search for the plaintiff with then cumbersome search engines (as opposed to just typing in the domain name).\textsuperscript{31}

In reaching its finding of dilution, however, the court recognized that neither it nor the district court relied on the traditional dilution forms of "blurring" or "tarnishment."\textsuperscript{32} Blurring occurs when a defendant uses a plaintiff's trademark to identify the defendant's goods or services, creating the possibility that the

\textsuperscript{25} Panavision, 141 F3d at 1324.

\textsuperscript{26} Id.

\textsuperscript{27} Id.

\textsuperscript{28} Id.

\textsuperscript{29} Panavision, 141 F3d at 1325-26 ("Toeppen's commercial use was his attempt to sell the trademarks themselves. Under the Federal Trademark Dilution Act and the California Anti-dilution statute, this was sufficient commercial use.").

\textsuperscript{30} Id at 1325 ("Toeppen's 'business' is to register trademarks as domain names and then sell them to the rightful trademark owners. He acts as a 'spoiler,' preventing Panavision and others from doing business on the Internet under their trademarked names unless they pay his fee.") (quotations omitted).

\textsuperscript{31} Id at 1327.

\textsuperscript{32} Id at 1326-27 ("To find dilution, a court need not rely on the traditional definitions such as 'blurring' and 'tarnishment.' Indeed, in concluding that Toeppen's use of Panavision's trademarks diluted the marks, the district court noted that Toeppen's conduct varied from the two standard dilution theories of blurring and tarnishment. The court found that Toeppen's conduct diminished 'the capacity of the Panavision marks to identify and distinguish Panavision's goods and services on the Internet.'").
mark will lose its ability to serve as a unique identifier of the plaintiff's product. Tarnishment occurs when a famous mark is improperly associated with an inferior or offensive product or service. As explained above, cybersquatting creates a different harm from blurring or tarnishment by diminishing mark holders' abilities to identify and distinguish their goods and services on the internet.

In applying anti-dilution laws thusly to prevent cybersquatting, courts were forced to map dilution analysis onto harms that were distinct from standard dilution harms. Toeppen's actions formed an easy case for the court to find dilution. The egregious facts satisfied dilution's commercial use requirements; Toeppen's serial registration of over one hundred famous marks as domain names and his repeated attempts to sell those domain names to the mark owners clearly showed a commercial business model premised on free riding others' trademark rights. However, the Panavision court provided little, if any, guidance for prospective efforts to prevent closer cases of less brazen cybersquatting.

For instance, even though the harm created by typosquatting is ostensibly the same as that created by Toeppen's brand of cybersquatting, the court may have inadvertently condoned typosquatting. In distinguishing a case relied upon by Toeppen, in which trademark infringement was not found against a defendant who obtained the most frequently misdialed phone number of plaintiff's "vanity number" in an attempt to capitalize on consumer confusion, the Panavision court noted that the slight misspelling did not constitute "use" of the plaintiff's mark. While

33 Panavision, 141 F3d at 1326 n 7. Following 2006 amendments to the dilution provisions of the Lanham Act, "dilution by blurring" is statutorily defined as "is association arising from the similarity between a mark or trade name and a famous mark that impairs the distinctiveness of the famous mark." 15 USC § 1125(c)(2)(B).

34 Id. Following 2006 amendments to the dilution provisions of the Lanham Act, "dilution by tarnishment" is statutorily defined as "association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark." 15 USC § 1125(c)(2)(C).

35 Panavision, 945 F Supp at 1304 (finding that defendant's cybersquatting diminished "the capacity of the Panavision marks to identify and distinguish Panavision's goods and services on the Internet").

36 Panavision, 141 F3d at 1319 ("Toeppen has registered domain names for various other companies including Delta Airlines, Neiman Marcus, Eddie Bauer, Lufthansa, and over 100 other marks. Toeppen has attempted to 'sell' domain names for other trademarks such as intermatic.com to Intermatic, Inc. for $10,000 and americanstandard.com to American Standard, Inc. for $15,000.").

37 Id at 1325. Toeppen relied on Holiday Inns, Inc v 800 Reservation, Inc, 86 F3d 619 (6th Cir 1996). The Panavision court explained: "Holiday Inns is distinguishable. There, the defendant did not use Holiday Inns' trademark. Rather, the defendant selected the
the Panavision court recognized that a domain name is generally different from a numerical phone number, it considered vanity phone numbers and domain names to be similar in that both use words to identify source. Accordingly, under Panavision’s imprecise treatment of domain names, typosquatting might not have constituted trademark use of a plaintiff’s mark, as typosquatting involves slight misspellings of such marks. Even though consumers can be confused by slight misspellings of domain names, foreclosing typosquatting from trademark use possibly excepted a large subset of likely confusing domain name registrations from enforcement. This incomplete and uncertain application of trademark law to infringing domain name registrations was unstable because it did not effectively map the needs of trademark holders onto the nuances and difficulties of the internet.

Toeppen shows that dilution analysis was the wrong vehicle for addressing typosquatting. Initially conceived, dilution protection was supposed to be available as a source of added protection beyond standard trademark infringement to a small number of highly famous marks. There was no federal anti-dilution statute prior to 1996, during which time trademark owners fought dilution with an uneven patchwork of state laws. The Federal Trademark Dilution Act of 1995 (“FTDA”), enacted January 16, 1996, created a federal cause of action for dilution. At least one prominent trademark commentator considered dilution protection under the FTDA too expansive. Thomas McCarthy wrote that, “Under the 1996 Federal Act, too many courts did not take the ‘fame’ requirement seriously and elevated to the ‘famous’ category marks that surely did not belong there,” adding that dilution became an overused cause of action. Dilution protection was not reined in until the Trademark Dilution Revision Act of 2006, so anti-cybersquatting enforcement was left to inconsistent judicial treatment under a dilution rubric that was stretched from its conceptual underpinnings through the middle

---

38 Panavision, 141 F3d at 1319.
and late 1990s. Relief arrived in 1999 with the enactment of the Anticybersquatting Consumer Protection Act.

A. ACPA Statute

Perceiving a rise in cybersquatting and amidst the uncertain judicial backdrop described above, Congress passed the Anticybersquatting Consumer Protection Act ("ACPA") in 1999.\textsuperscript{42} The ACPA created a statutory tort for cybersquatting, setting out the standard that anyone who, with "bad faith intent to profit,"\textsuperscript{43} "registers, traffics in, or uses a domain name"\textsuperscript{44} that is a recognized trademark at the date of registration,\textsuperscript{45} is liable of cybersquatting.\textsuperscript{46}

By explicitly barring cybersquatting, the ACPA obviated convoluted reliance on dilution theories to enforce protection from cybersquatting and made private anti-cybersquatting enforcement much easier.\textsuperscript{47} Rather than collapsing dilution analysis into a determination of commercial use, the revised § 43(d) offers a non-exhaustive list of nine factors that courts may use to determine bad faith intent to profit.\textsuperscript{48} The factors allow courts to

\textsuperscript{43} 15 USC § 1125(d)(1)(A)(i).
\textsuperscript{44} 15 USC § 1125(d)(1)(A)(ii).
\textsuperscript{46} 15 USC § 1125(d)(1)(A).
\textsuperscript{47} See generally Panavision, 141 F3d at 1316; Intermatic Inc v Toeppen, 947 F Supp 1227 (N D Ill 1996).
\textsuperscript{48} 15 USC § 1125(d)(1)(B)(i). The nine non-exclusive factors for determining a person's bad faith intent to profit are: 1) the trademark or other intellectual property rights of the person, if any, in the domain name; 2) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person; 3) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services; 4) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name; 5) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site; 6) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct; 7) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct; 8) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of
consider aspects mitigating bad faith intent to profit, such as a cybersquatting defendant's noncommercial or fair use, prior use of the contested name in selling goods or service, and any other intellectual property rights to use the contested domain name. Factors that tend towards findings of bad faith intent to profit include a defendant's: intent to divert consumers from the mark owner's online location to a site accessible under the domain name; offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct; provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct; and registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others. Additionally, the ACPA allows cybersquatting enforcement for any distinctive mark, which relaxed the higher famousness requirement necessary for enforcement under dilution.

In registering websites with ICANN, registrars report the contact information of their domain name registrants by submitting the information into the Whois database. The database serves as an efficient means of ensuring transparency and accountability online by making website operators immediately accessible in the real world. The case law prior to the ACPA held that the then sole registrar, Network Solutions, Inc. ("NSI"), could not be liable for registering domain names to alleged cybersquatters. The ACPA granted domain name registrars safe harbor from liability for registering an infringing domain name and for refusing to register, canceling, or transferring a domain name in furtherance of a dispute resolution policy. However, this statutory safe harbor does not explicitly protect other ser-

---

52 15 USC § 1125(d).
vices, such as hidden Whois.\textsuperscript{53} Hidden Whois services offered legitimate benefits to early domain name registrants, by diverting massive amounts of computer generated spam email and phishing attacks directed at Whois database registrants to registrars' shell email addresses.\textsuperscript{54} Today, though, advances in spam filtering technologies have mooted this justification for hidden Whois services' continued existence.\textsuperscript{55} It is suspected that the foremost remaining purpose served by hidden Whois services is to obscure the identities of domain name registrants. While some percentage of registrants surely wish to avoid disclosing their identities in the public Whois database purely for privacy reasons, scores of registrants operating infringing domain names hide their identities to evade prosecution.

II. ESTABLISHING THE CASE FOR REGISTRAR LIABILITY

In light of the present state of domain name registration discussed above, this Part establishes the basis for domain name registrar liability for registrants' illegal websites when hidden Whois services are employed. This argument explains both the legal justifications and policy rationales that support the proposed liability rule.

The problem to be solved is this: opportunistic domain name registrars offer additional services to registrants that effectively hide the identity and contact information of their domain name registrant customers. The effect of these hidden Whois services is to stifle accountability when registrants operate illegal websites or own infringing domain names. Under the current arrangement, in which vacuous and inaccurate registrar information appears in the Whois database in registrants’ stead, aggrieved plaintiffs must expend resources drafting demand letters to or complaints against registrars to secure the true identities of defendant registrants. Hidden Whois services create unnecessary barriers to enforcing registrant liability and accountability, thus raising plaintiffs’ costs of private enforcement while simultaneously creating revenues for domain name registrars. Plaintiffs could rely upon agency principles to hold registrars liable for registrants’ infringing websites under existing trademark laws.

\textsuperscript{53} Id.


\textsuperscript{55} NSI's Hidden Whois accommodates both ends, by preventing spam and allowing for registrant accountability.
The proposed liability rule would serve as a middle ground between the current regime of tacit tolerance of hidden Whois services on one side and an outright ban of all hidden Whois services on the other: it would allow injured plaintiffs to efficiently pursue the actual domain name owner or, if different, the party that appears as registrant in the Whois database. This would provide tort victims with clear access to remedies, and any resulting damages could be shifted between registrar and registrant by contract thereafter. ICANN and the Whois database set public disclosure of registrant identity as the default. Those registrants interested in keeping their identities private when registering domain names would not be barred from doing so, but would instead have to pay a presumptively higher registration fee to buck the default rule by asking registrars to assume the risk of their liability. In these ways, as explained below, the proposed rule accommodates the interests of registrars, registrants, and trademark owners.

A. Legal Basis for the Availability of Registrar Liability under Existing Law

The legal argument for allowing liability to fall to registrars operates within the space of the Lanham Act's anti-cybersquatting provisions. This section of the Act outlaws the registration, traffic in, and use of domain names that are identical or confusingly similar to another's trademark, when such actions are made with bad faith intent to profit. This prohibition encompasses both cybersquatting, which is the registration of a domain that is identical to another's trademark, and typosquatting, which is the registration of a domain name that is confusingly similar to another's trademark. The Act provides that domain name registrars operating in their standard capacities as registrars are essentially free from liability for the registration and maintenance of registrants' illegal websites. However, by applying agency principles to the registrar/registrant relationship, the Lanham Act's anti-cybersquatting provisions could be interpreted to find liability in registrars who offer hidden Whois services for illegal websites. The way to achieve such a result

---

56 15 USC § 1125(d).
57 Id.
58 15 § 1125(d) prohibits the use of both identical and confusingly similar domain names.
59 15 USC § 1114(2)(D)(iii).
would be to expose to liability as registrant both true owners of infringing domain names as well as any party appearing as registrant in the Whois database. Thus, by inserting their identities into the Whois database when offering hidden Whois services, domain name registrars could be judged as registrant for having created the cybersquatting harm.


The ACPA created a statutory tort that allows trademark owners to sue only a “domain name registrant or that registrant’s authorized licensee,” if such person “registers, traffics in, or uses a domain name” in ways likely to create confusion and with bad faith intent to profit from the mark.

As explained above, domain name registrars generally are immune from liability under the ACPA. “[A] registrar who simply accepts the registration of a domain name generally is not liable for trademark infringement or dilution, unfair competition, or violations of the ACPA.” Thus far, courts have not required registrars to act as gatekeepers that prevent the registration of trademark terms as domain names and have not found registrars allowing such infringing registrations to constitute “bad faith intent to profit” from marks. However, no federal court has considered whether the sale of hidden Whois services can open a registrar to liability under the ACPA, and no court to date has applied the ACPA to instances in which the registrar appears as a registrant in the Whois database.

Registrars that appear in the Whois database in fulfillment of hidden Whois service obligations ought to be treated as registrants for liability purposes under the ACPA. As explained in *Lockheed Martin Corp v Network Solutions, Inc*, the registrars are immune from liability when acting in their normal capacities as registrars. The problem is that registrars offering hidden Whois services are acting well past their typical roles as registrars by standing in the place of registrants in the Whois data-

---

60 15 USC § 1125(d)(1)(D).
61 15 USC § 1125(d).
62 See, for example, *Lockheed Martin Corp v Network Solutions, Inc*, 141 F Supp 2d 648 at 655 (finding that 15 USC § 1125(d) does not give a cause of action against domain name registrars acting in their standard capacities).
64 See id; *Lockheed Martin*, 141 F Supp 2d at 656.
65 *Lockheed Martin*, 141 F Supp 2d at 655.
base. Additionally, registrars tacitly recognize that the hidden Whois service is one that extends beyond standard registrar function, as illustrated by registrars charging additional fees for the service above the baseline charge for the standard bundle of registration services. Registrars offering hidden Whois services stand in the place of their registrant customers in the Whois database, obfuscating the true identities of domain name owners for additional fees. The nature of this exceptional service justifies precluding registrars that inject themselves into the Whois database from the general grant of registrar immunity.

2. Agency principles.

An agency argument could operate as a theory of liability to find registrars that offer hidden Whois services and appear as registrants in the Whois database liable for registrants' illegal websites. Registrars offering hidden Whois services operate as agents for registrants by virtue of the formers' appearance as registrants in the Whois database. The registrants are undisclosed principals in this agency arrangement, as prospective plaintiffs cannot know registrants' true identity and are only able to make contact with the agent registrars. By charging extra for the hidden Whois service, the registrar is acting in a capacity beyond that of standard registrar, standing in the stead of the registrant for purposes of the Whois database. Accordingly, under this agency theory, any liability growing out of that registration can fall upon the registrar, because the registrar can be treated as the party causing cybersquatting harm by virtue of its designation as domain name owner in the Whois database. Here, liability that would ordinarily fall only upon the registrant by virtue of an infringing domain name registration can also rest with the registrar. By serving as the undisclosed principal's agent, the registrar assumes the risk of liability created by the website or its illegal domain name registration.

Conceding that the ACPA did not create new causes of action against domain name registrars acting in their standard capacities, a plaintiff seeking to recover against a domain name regis-

---

66 Restatement (Third) of Agency § 1.04(2)(b) (cited in note 4).
67 See Lockheed Martin, 141 F Supp 2d at 655. As explained elsewhere in this Comment, Congress and the courts have not required registrars to serve as gatekeepers when acting in their normal capacities registering customers' domain names. The law provides no cause of action against registrars registering domain names in their standard capacities; however, this Comment argues that registrars that insert themselves into the role of registrant in the Whois database through hidden Whois services are acting beyond their
HIDDEN WHOIS AND INFRINGEMENT DOMAINS

The registrar could still assert that the registrar served as the agent for the unknown registrant by appearing as the registrant in the Whois database and that this action opens the door for registrar liability. Essentially, the registrar would be made to stand in the registrant's shoes because it acted as registrant in the Whois database in a capacity exceeding the standard role of a typical registrar.

The cause of action is the registrant's violation of the ACPA, and the registrar could be found liable for that violation by virtue of its relationship with the registrant. Registrars offering hidden Whois services operate as agents to the undisclosed principals who are the registrants of infringing domain names. Aggrieved plaintiffs alleging infringement under the Lanham Act are third parties to the arrangement, whose rights are alleged to have been infringed under the ACPA. The proposed liability rule would come into force only when the registrant would otherwise be liable for infringement and the registrar has hidden that registrant's identity and contact information from the Whois database. Thus, registrars offering hidden Whois services for noninfringing domain names would not be liable because no underlying infringement would exist, while those registrars offering hidden Whois services for infringing domain names would be liable.

The Restatement (Third) of Agency explains:

An agent is subject to liability to a third party harmed by the agent's tortious conduct. Unless an applicable statute provides otherwise, an actor remains subject to liability although the actor acts as an agent or an employee, with actual or apparent authority, or within the scope of employment.68

Accordingly, once a court accepts that the registrar is serving as the registrant by virtue of the former's appearance in the Whois database, the registrar will not be able to escape liability under agency law principles, unless the registrar can find and rely upon some constitution, statute, regulation, or ordinance to exempt its actions from liability.69

The Restatement section stands for the principle that an agent is responsible for the torts he commits. The registrar's tortious conduct is the cybersquatting violation for which it would

standard capacities as registrars and ought to be subject to liability.

68 Restatement (Third) of Agency § 7.01 (cited in note 4).
69 Id.
be responsible by virtue of appearing as the infringing domain name's owner. The comments to the Restatement elaborate:

An agent whose conduct is tortious is subject to liability. This is so whether or not the agent acted with actual authority, with apparent authority, or within the scope of employment... The justification for this basic rule is that a person is responsible for the legal consequences of torts committed by that person. A tort committed by an agent constitutes a wrong to the tort's victim independently of the capacity in which the agent committed the tort. The injury suffered by the victim of a tort is the same regardless of whether the tortfeasor acted independently or happened to be acting as an agent or employee of another person.70

In short, the agent's conduct makes it liable for its tortious actions, independent of its relationship to a principal. This further suggests that even if a registrar released the identities of the true domain name registrants, thereby disclosing the identities of previously undisclosed principals in this agency scheme, the registrar's liability to third party plaintiffs for its tortious cybersquatting would not disappear. Once courts recognize registrars offering hidden Whois services as agents of registrant principals, this logic results in prospective plaintiffs being able to hold registrars liable as defendants at the outset of litigation, thus obviating the need for plaintiffs' to issue repeated demands for registrant information prior to filing a complaint.

While United States federal law reflects examples of agency exemptions from liability for distinguishable agents performing distinguishable activities, no federal statutory exemption or privilege could be found to successfully relieve registrars of their liability in this context.71 For certain actions, federal law specifically exempts domain name registrars from liability. For example, domain name registrars acting as such are not subject to liability for providing the Federal Trade Commission with information relevant to unfair or deceptive practices or assets subject to recovery by the Commission.72 Such registrar action is distinguishable from the registrar action contemplated in this Com-

70 Id at comment b.
71 Restatement (Third) of Agency § 7.01 (cited in note 4) (requiring such statutory exemption in order for agency liability to be broken).
72 15 USC § 57b-2b (Supp 2006).
ment, as the former action is taken to assist in law enforcement efforts and government investigations, while the latter obscures private enforcement of federal trademark law. Further, the United States Code contains laws exempting certain classes of agents. For example, the Federal Tort Claims Act exempts agents of the United States government from individual liability for torts committed while exercising due care in the execution of a statute or regulation or while performing a discretionary function or duty on the part of a federal agency. The specific principal-agent relationship exempted by this statute is distinguishable from the registrar-registrant agency relationship in which registrars offering hidden Whois services engage. Because no comparable statutory exemptions exist that could apply to such registrars, agent liability for their tortious activity will not be severed. Furthermore, courts have applied the agency law principle that agents are individually liable for their own torts in federal trademark, patent, copyright, and unfair competition cases.

B. Remedies

Under the existing trademark statutes, registrars' liability could rise to the level of damages when offering hidden Whois services. The remedies section of the Lanham Act explains that:

A domain name registrar, a domain name registry, or other domain name registration authority shall not be liable for damages under this section for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name.

74 Restatement (Third) of Agency § 7.01 (cited in note 4).
75 See Donsco, Inc v Casper Corp, 587 F 2d 602, 606 (3d Cir 1978) (liability to competitor under Lanham Act, 15 USC § 1125(a), for acts of unfair competition; corporate officer who authorized and approved acts of unfair competition is subject to individual liability); Dixon v Atlantic Recording Corp, 1985 WL 3049 at *2 (S D NY 1985) (collecting and licensing agent for owner and publisher of song “Whole Lotta Love” subject to individual liability in copyright infringement action brought by copyright owner of song; apart from “intricacies of agency law,” a person “who promotes or induces an infringement can be held liable as a ‘vicarious infringer,’ even though he has no actual knowledge that a copyright is being violated, if (1) he has the right and ability to control or supervise the infringing activity, and (2) he has a direct financial interest in the exploitation of the copyrighted materials”).
76 15 USC § 1114(2)(D)(iii) (emphasis added).
Accordingly, a domain name registrar's bad faith intent to profit must be established for damages to be levied against it. 15 USC § 1125(d)(1)(B) sets out nine non-exclusive factors that may be considered by courts in determining the requisite bad faith intent to profit.77 Realizing that domain name registrars receive extra fees for providing hidden Whois services and that such services inaccurately reflect registrants' information in the Whois database, the following factor in the test for bad faith should be applied to registrars:

[T]he person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct.78

Hidden Whois services fall squarely within the forms of questionable action contemplated by this factor. Registrars are intentionally providing ICANN and the Whois database with incorrect registrant information when they submit their own contact information in place of the registrants'. In doing so, registrars are creating extra profits, and, even though they are not the registrant, such registrars are essentially trafficking in domain names that may be illegal.

In a case dealing with registrar liability, the Lockheed Martin court found that § 1114(2) does not create new causes of action but is merely intended to limit liability.79 Because liability already can lie in registrars through the agency principles explained above, a separate cause of action against registrars is not required for them to be liable for damages when offering hidden Whois services. Rather, the statutory cause of action that exists against registrants in § 1125(d) can be used to find liability in registrars, as registrars offering hidden Whois services would be made to stand in the role of registrant. This liability is not limited to injunctive liability; it can rise to the level of damages due to registrars' bad faith intent to profit from offering additional and misleading hidden Whois services.80

77 15 USC § 1125(d)(1)(B).
79 Lockheed Martin, 141 F Supp 2d at 655. Note that this case dealt with cybersquatting in the general context as opposed to a registrar providing hidden Whois services.
80 See 15 USC § 1114(2).
While the Lanham Act's remedies provision may preempt a registrar's exposure to damages, it likely will not exempt the registrar if a court finds that appearing as registrant in the Whois database allows the registrar to be considered as registrant in litigation under agency law principles.81

C. Benefits of a Registrar Liability Rule

Endorsing the proposed liability rule against domain name registrars offering hidden Whois services would have numerous salutary effects. If courts adopt such a rule, then registrars' costs of offering hidden Whois services that shield registrants' identities would rise due to registrars' increased exposure to liability. This would result in more expensive hidden Whois services, which would reduce registrant demand for such services. Such a decline in hidden Whois services would make the Whois database a more accurate and useful tool for ascertaining true website owners. This, in turn, would allow for cheaper and easier private enforcement of anti-cybersquatting laws. Prospective plaintiffs would be able to serve defendants with complaints on the first attempt, relying confidently upon the information listed in the Whois database. Under this rule, plaintiffs would not have to take costly steps procuring registrants' actual information from registrars who have hidden registrants' information from the Whois database.

Further, registrars would respond to increased exposure to liability by offering legally preferable services that do not obscure registrants' identities. For instance, registrar Network Solution, Inc.'s ("NSI") hidden Whois service operates in an acceptable manner that is distinct from those hidden Whois services intended to be subject to the proposed registrar liability rule. With its Private Domain Name Registration service, NSI enters alternate contact information in the Whois database, but makes public registrants' true identities and employs email masking technologies to filter spam and automatically forward genuine emails to registrants' private addresses.82 For each domain name, NSI creates an alternate email address that appears publicly in the Whois database. Legitimate, non-spam email is for-

81 See Lockheed Martin, 141 F Supp 2d at 655 (finding that 15 USC § 1114(2) only limits available remedies, but does not affect causes of action).

warded to registrants' privately maintained email addresses. The NSI service is distinguishable from the evasive hidden Whois services contemplated in this Comment in two respects: 1) prospective plaintiffs can effectively and directly contact the domain name registrants that use NSI's service; and 2) registrants' true identities appear publicly in the Whois database. NSI does not hide domain names' true owners. To the extent that registrants purchase hidden Whois services in good faith to prevent spam, we would expect to see registrars offer and registrants purchase preferable services like NSI's.

The proposed liability rule would create additional efficiencies in instances in which a prospective plaintiff believes it has causes of action against multiple infringing domain name registrations. For instance, if a single registrar registers multiple domain names that are confusingly similar to a plaintiff's mark to multiple typosquatting registrants that use the registrar's hidden Whois service, then, under the proposed liability rule, the plaintiff would only have to file one suit against the registrar in order to protect its mark. This would be far less costly than pursuing several unknown registrants, whose identities are hidden, in separate actions. Additionally, by allowing the aggregation of causes of action into a single complaint against a registrar, registrars that are notorious for registering illegal domain names will be held accountable for their role in facilitating illegal domain name registration.

Rather than bringing suit against an unknown number of unidentifiable defendants, plaintiffs should be able to bring a single suit against a domain name registrar for all of the allegedly infringing domain names that it has registered that employ the registrar's hidden Whois service. Agency law principles could be used to extend registrant liability to registrars. That liability would not disappear even if registrars disclose the websites' actual registrants. While this position reflects a definite movement away from the complete immunity from liability enjoyed by NSI when it was the only authorized registrar, the proposed liability rule would serve as a check on today's competing registrars from offering services that make illegal activity harder to prevent.

Another nuanced benefit of the proposed liability rule is that it stands as middle ground that accommodates privacy interests. To the extent that that domain name owners are concerned with exposing their identities for sincere privacy reasons, the proposed rule is advantageous because it stops far short of outlawing hidden Whois services altogether. Rather, it merely sets a
starting point from which domain name owners and registrars could negotiate for hidden Whois services that do not impose externalities on third party trademark owners. For instance, a domain owner that is unwilling to expose its identity to the Whois database when registering a domain name could include an indemnity term with its registrar in their registration contract. The indemnity would contemplate the hidden registrant reimbursing the registrar for any tort damages the registrar incurs by virtue of the latter's appearance in the Whois database. In this manner all interests would be served: the registrant's privacy would be maintained, the registrar would be able to earn a fee for service and its liability would be recompensed, and any aggrieved trademark owner would be able to effectively and efficiently ascertain the tortious actor from the Whois database. This solution is superior to the present condition, in which hidden Whois is tolerated unchecked, as tort victims will receive clear paths to efficient recovery.

III. CONCLUSION

This Comment addresses the difficulties hidden Whois services pose to enforcing anti-cybersquatting laws. By using hidden Whois services, domain name registrants are able to evade accountability for their ownership of infringing domain names. Registrars that presently offer hidden Whois services do so in a drastically different technological landscape from the one that existed a decade ago. Whereas the hidden Whois service of years past offered a legitimate service to registrants, today's hidden Whois stifles private enforcement of trademark laws. This Comment sets out an approach that can be used by potential plaintiffs to enforce liability against domain name registrars for the tortious actions of the registrants they protect. By posing as registrants in the Whois database, registrars are acting beyond their standard roles and ought to be made available to liability when their actions obscure a plaintiff's attempts to enforce his rights. By creating a default liability rule for registrars offering hidden Whois services, the framework proposed in this Comment serves as an efficient middle ground between continuing to allow registrars to undermine the integrity of the Whois database on the one hand and completely banning hidden Whois services altogether on the other. Whether prospective courts read the proposed approach into existing trademark law by interpretation or Congress amends existing law to explicitly reflect the proposed approach, adopting the liability rule discussed in this Comment
would help trademark owners enforce their rights and would be a step in the direction of promoting lawful electronic commerce.