UIC Law Review

Volume 38 | Issue 1 Article 13

Fall 2004

Balancing Individual Privacy Rights and the Rights of Trademark Owners in Access to the WHOIS, 38 J. Marshall L. Rev. 357 (2004)

Jeffrey Stephen Sobek

Follow this and additional works at: https://repository.law.uic.edu/lawreview

 Part of the Computer Law Commons, Consumer Protection Law Commons, Intellectual Property Law Commons, Internet Law Commons, Marketing Law Commons, and the Privacy Law Commons

Recommended Citation

Jeffrey Stephen Sobek, Balancing Individual Privacy Rights and the Rights of Trademark Owners in Access to the WHOIS, 38 J. Marshall L. Rev. 357 (2004)

https://repository.law.uic.edu/lawreview/vol38/iss1/13

This Comments is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC Law Review by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

BALANCING INDIVIDUAL PRIVACY RIGHTS AND THE RIGHTS OF TRADEMARK OWNERS IN ACCESS TO THE WHOIS

JEFFREY STEPHEN SOBEK*

INTRODUCTION

"During much of the 1990's, the Internet was like the old west. There were those who saw, and many who still see, the Internet as a wide expanse of land that should be free for anyone to exploit in any manner one sees fit."[1] However, just as it was necessary to "bring order to chaos"[2] in the Wild West as the population increased, the explosive growth of the Internet has brought with it the need to protect the rights and interests of the on-line population.[3] Regulation of the WHOIS database, which is the registration database for all domain names, is one of the most controversial Internet issues today.

Part I of this Comment lays a foundation for the understanding of various technical aspects of the Internet, including the way in which information is stored and located making it possible for the Internet to be an effective medium for research. Part II explores the way in which the constitutionally protected rights of privacy and intellectual property are affected by allowing public access to the WHOIS database. Part II also addresses the pros and cons of requiring registrants of domain names to provide accurate information, and requiring users querying the WHOIS to provide accurate identification. Part III

---

* J.D., January 2005, The John Marshall Law School. The author wishes to thank adjunct professor Robert Gurwin for his help with the topic, the author's family for their invaluable support, and the John Marshall Law Review Board and Candidates for their editorial work.

1. Jeffrey J. Look, *Law and Order on the Wild, Wild West (WWW)*, 24 U. ARK. LITTLE ROCK L. REV. 817, 817 (2002).

2. *Id.*

3. *See* Catherine T. Struve & R. Polk Wagner, *Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act*, 17 BERKELEY TECH. L.J. 989, 990 (2002) (suggesting the Internet will present new challenges to the scope and enforcement of laws). The way in which countries respond to the new challenges "will have far-reaching implications for the ordering of social and economic behavior online." *Id.*

proposes that the WHOIS should continue to be accessible to the public, but that the administration of the WHOIS and the domain name registration process must be changed so that domain name registrants and those who access the WHOIS will be held accountable if they violate the rights of others.

I. INTERNET BASICS

A. Design and Proliferation of the Internet

The Internet can best be described as a network of internationally interconnected computers.[4] Use of the Internet is growing at an astounding pace.[5] It is estimated that there are over 605 million Internet users worldwide.[6] Commerce on the Internet is expected to surpass $2.7 trillion by the end of 2004.[7]

Generally, an individual accesses the Internet via a host computer.[8] Every host computer has an identifier, which is a unique sequence of numbers called an Internet Protocol address ("IP address").[9] The IP address associated with each host computer enables other computers to identify and locate it.[10] Computers use IP addresses to route every transmission that

---

4. *See* Reno v. ACLU, 521 U.S. 844, 849-50 (1997) (describing design of Internet and stating that by 1996, the Internet was comprised of approximately 9.4 million computers). *See also* GlobalSantaFe Corp. v. GlobalSantaFe.com, 250 F. Supp. 2d 610, 618 (E.D. Va. 2003) (explaining the computers making up the Internet are located all over the world and each computer has a unique identifier); Thomas v. Network Solutions, Inc., 176 F.3d 500, 502 (D.C. Cir. 1999) (explaining the backbone of the modern Internet developed from a network the United States military developed for research and education).

5. *See* DEBORAH E. BOUCHOUX, INTELLECTUAL PROPERTY: THE LAW OF TRADEMARKS, COPYRIGHTS, PATENTS, AND TRADE SECRETS 110 (2000) (describing the effects the explosive popularity of the Internet has had on issues affecting intellectual property rights).

6. Nua Internet Surveys, *How Many Online?*, *at* http://www.nua.ie/surveys/how_many_online/ (Sept. 2002).

7. Press Release, Nua Internet Surveys, eMarketer: Worldwide B2B Revenues to Pass One Trillion (Apr. 1, 2003), *at* http://www.nua.ie/surveys/?f=vs&art_id=905358753&rel=true (last visited Sept. 14, 2004). Seventy percent of companies have experimented with purchasing online. *Id.*

8. *See Reno*, 521 U.S. at 850 (defining a host computer as one that "store[s] information and relay[s] communications").

9. *See Thomas*, 176 F.3d at 503 (describing an Internet Protocol address as "four numbers, each between 0 and 255, separated by periods. . . . The first number signifies the computer's geographic region; the second number a specific Internet Service Provider; the third a specific group of computers; and the fourth a specific computer within that group"); G. Peter Albert, Jr., *Eminent Domain Names: The Struggle to Gain Control of the Internet Domain Name System*, 16 J. MARSHALL J. COMPUTER & INFO. L. 781, 784 (1998).

10. *Thomas*, 176 F.3d at 502; 63 Fed. Reg. 8826 (Feb. 20, 1998) (to be codified at 15 C.F.R. pt. 23).

passes through the Internet.[11] Because it would be difficult for a person to remember many different IP addresses, the Internet community devised the domain name system ("DNS").[12] The DNS assigns each computer an easy-to-remember alphanumeric name,[13] such as "jmls.edu,"[14] instead of a numerical IP address, such as "192.207.162.0." This alphanumeric name is called a domain name. The DNS essentially "links" every unique domain name to a corresponding, unique IP address.[15] Although it is the domain name that most people use to access a particular website, it is actually the IP address associated with the particular domain name that connects users to the computer hosting the website.[16]

B. The Domain Name System

The DNS is a "hierarchical and distributed system," meaning that there is no master file located in any single geographical location that stores every registered domain name.[17] Rather, the information matching domain names to IP addresses is stored on

---

11. *GlobalSantaFe*, 250 F. Supp. 2d at 618.

12. Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295 (1998).

13. *GlobalSantaFe*, 250 F. Supp. 2d at 618 n.19 (citing *Thomas*, 176 F.3d at 503 n.1)

> The DNS offers additional benefits beyond providing an easier-to-remember naming system. Among other benefits, it allows changes at the host computer or Internet Service Provider (ISP) level without individual user confusion or disruption. For example, a change in a host computer's ISP generally necessitates a change in the IP address of that computer. In such situations, the individual user can continue using the same domain name, unaware that the corresponding IP address of the host computer has been changed.

Id.

14. The user DNS servers for The John Marshall Law School contain the addressing information for the machines relating to jmls.edu, the John Marshall Law School assigned domain name.

15. *See Thomas*, 176 F.3d at 503 (explaining that in order for the DNS to function properly, "each domain name must be unique and correspond to a unique Internet Protocol number"). *See also* PGMedia Inc. v. Network Solutions, Inc., 51 F. Supp. 2d 389, 390-91 (S.D.N.Y. 1999) (explaining the technical aspects of the DNS); Strick Corp. v. Strickland, Jr., 162 F. Supp. 2d 372, 373 n.1 (E.D. Pa. 2001) (explaining a domain name enables a user to find a specific location on the Internet, just as a street address or phone number allows a person to locate or contact a specific person or business); *Thomas*, 176 F.3d. at 503 (explaining "a domain name is not an address as typically understood but instead is a mark identifying a specific person's or organization's site on the Internet"). Therefore, because there is no association between a domain name and the physical location of a computer, the physical location of the computer can be moved while the domain name remains the same. *Id.*

16. Chatam Int'l, Inc. v. Bodum, Inc., 157 F. Supp. 2d 549, 553 (E.D. Pa. 2001).

17. *GlobalSantaFe*, 250 F. Supp. 2d at 618.

Internet-connected computers located around the world.[18] "Under this hierarchical system, the domain name 'space' is divided into top-level domains ("TLD's") and second-level domains ("SLD's")."[19] A TLD[20] name server contains all of the information necessary to direct a domain name query to the SLD[21] name server responsible for the domain name being queried.[22] The SLD name server, in turn, maintains the necessary information to match a domain name query to the individual computer hosting the corresponding IP address.[23]

The process by which a computer is assigned an IP address is separate from the process by which a domain name is registered.[24] The Internet Service Provider ("ISP") providing a particular computer's Internet connection usually assigns that computer its IP address.[25] Domain names, on the other hand, must be requested from a domain name registrar[26] such as Register.com[27]

---

18. *See Thomas*, 176 F.3d. at 503 (describing the process in which domain names and IP addresses are used to locate Internet computer sites).

19. *See GlobalSantaFe*, 250 F. Supp. 2d at 618 (explaining how a domain name query is routed through the domain name system to the computer hosting the corresponding website).

20. *See* Cable News Network, L.P. v. CNNews.com, 162 F. Supp. 2d 484, 486 n.4 (E.D. Va. 2001) (explaining for each TLD there is a single organization responsible for maintaining the database of every domain name in that TLD). *See also* Internet Corporation for Assigned Names and Numbers, *Top-Level Domains, at* http://www.icann.org/tlds (last visited Sept. 15, 2004) (listing and defining the top level domains currently available); *see also GlobalSantaFe*, 250 F. Supp. 2d at 619 n.20 (listing available TLDs, which include ".com," ".net," ".org," ".edu," ".gov," ".int" ".mil," ".biz," ".info," ".name," ".pro," and more than 240 "country-code" TLDs, such as ".us" for the United States).

21. The secondary level domain is "the part of the domain name to the left of the period," such as "jmls" in "jmls.edu." BOUCHOUX, *supra* note 5, at 477.

22. *GlobalSantaFe*, 250 F. Supp. 2d at 618.

23. *Id.* at 618-19.

> [For example], VeriSign, as the registry for all domain names ending in ".com" is responsible for directing domain name queries regarding the "globalsantafe.com" second level domain to the appropriate SLD name server. This SLD name server, in turn, matches the domain name, e.g. "www.globalsantafe.com," with its specific numeric IP address. In other words . . . the ."com" zone linked to the IP addresses of the SLD name servers for those second level domains, while the "globalsantafe.com" SLD name server maintains the file which matches all domain names in the "globalsantafe.com" SLD zone to the IP addresses of the individual host computers.

Id.

24. *Id.* at 618 n.18.

25. *See id.* (noting IP addresses are allocated in blocks to ISPs "by one of the four Regional Internet Registries, such as the American Registry for Internet Numbers [("ARIN")]"). To find more information about the services provided by ARIN see the American Registry for Internet Numbers at http://www.arin.net/registration (last visited Sept. 14, 2004).

26. *See* Schmidheiny v. Weber, 319 F.3d 581, 582 (3d Cir. 2003) (discussing the steps necessary for a person to obtain a domain name). *See also*

or Network Solutions, Inc.[28]

"Domain name registrars are organizations that keep track of Internet domain names and ensure that only one party controls a specific domain name during any given period."[29] The registrant, an individual or business interested in having the exclusive use of a domain name, must enter into a contractual agreement[30] with a registrar.[31] Registrars, in turn, are governed by several contracts between themselves and the registries.[32] A registry is responsible for the "central but more limited function" of maintaining the database of every domain name in a given TLD.[33] A registrar, in addition to its other duties, is responsible for maintaining "records containing the name and address of the registrant as well as information regarding a technical and administrative contact for each domain name."[34] This information pertaining to the registrant is available to the public via the WHOIS.[35]

Register.com, Inc. v. Domain Registry of Am., No. 02-6195, 2002 U.S. Dist. LEXIS 24795, at *3 (S.D.N.Y Dec. 26, 2002) (stating there are currently approximately 150 accredited registrars worldwide).

27. For information about registering a domain name with Register.com see the Register.com website at http://www.register.com (last visited Sept. 16, 2004).

28. For information about registering a domain name with Network Solutions, Inc. see Network Solutions, Inc.'s website at http://www.network solutions.com (last visited Sept. 16, 2004).

29. *See Schmidheiny*, 319 F.3d at 582 (citing Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187, 216-17 (2000)).

30. Registration service agreements generally require the registrant to agree to certain terms and conditions and to pay a specific amount of money "for the right to use the domain name for a fixed period of time." *Id.* To view examples of standard service agreements see http://www.register.com/service-agreement.cgi?cmp=IL10682 (last visited Sept. 29, 2004), as well as http://www.networksolutions.com/en_US/legal/static-service-agreement.jhtml (last visited Sept. 29, 2004).

31. *Schmidheiny*, 319 F.3d at 582. *See also* Fleetboston Fin. Corp. v. Fleetbostonfinancial.com, 138 F. Supp. 2d 121, 123 n.2 (D. Mass. 2001) (describing distinctions between registrars and registries).

32. *See GlobalSantaFe*, 250 F. Supp. 2d at 619 (describing the contractual relationship between a registrar and a registry). Contracts governing these entities include the Registry-Registrar Agreement, the Registrar Accreditation Agreement, and the .com Registration Agreement. *Id.* For a list of various agreements governing the registrar-registry relationship, see the ICANN registry agreement page at http://www.icann.org/registries/agreements.htm (last visited Sept. 16, 2004).

33. *See GlobalSantaFe*, 250 F. Supp. 2d at 619 (explaining the function of a registry is "maintaining and operating the unified Registry Database, which contains all domain names registered by all registrants and registrars in a given top level domain, as well as the associated TLD zone file used to resolve domain name queries in that domain").

34. *See id.* (describing the registrar's responsibilities as handling "the retail side of domain name registration, selling domain names to individual domain name registrants").

35. *See Register.com*, 2002 U.S. Dist. LEXIS 24795, at *4 (explaining that

C. Specifics of the WHOIS Database

The WHOIS "is a domain based research service containing the name, address, and technical information of each domain name registrant."[36] Every domain name registrar accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN")[37] is bound by the terms of the ICANN Registrar Accreditation Agreement ("RAA")[38] to maintain the WHOIS.[39] To both companies and consumers, "the WHOIS is an identifier" that can be used by a variety of individuals for a variety of purposes: by a businessman who wants to inquire about the availability for purchase of a specific domain name, by a parent who "wants to know who owns the website that is distributing harmful toys," by a consumer who "wants to know who owns the website that is offering discounted pharmaceuticals," or by a "trademark or copyright owner [who] wants to know who owns the domain name from which a counterfeit version of its products are being sold."[40] Any person with access to the Internet may access and search the

---

administrative and contact information pertaining to domain name registrants is listed in a database called "WHOIS" database).

36. Look, *supra* note 1, at 821 n.22.

37. ICANN is "an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions." ICANN, *ICANN Information, at* http://www.icann.org/general (last visited Sept.17, 2004).

38. *See The WHOIS: Privacy and Intellectual Property Issues: Hearing Before the Subcomm. on Courts, the Internet and Intellectual Property*, 108th Cong. 2 (2001) [hereinafter *Trainer Statement*] (statement of Timothy P. Trainer, President, International AntiCounterfeiting Coalition) (specifying types of information that registrars are required to provide in the WHOIS). Specifically, section II.F. of the RAA states that as long as the RAA agreement is in effect, every registrar must maintain an interactive web page that provides "free public query-based access to up-to-date (that is, updated at least daily)" information about every active domain name in the registry of each of the TLDs. *Id.* at n.2 The information that must be contained in the database is:

> The name of the SLD being registered and the TLD for which registration is being requested; (a) The IP addresses of the primary nameserver and secondary nameserver(s) for the SLD; (b) The corresponding names of those nameservers; (c) The identity of Registrar . . .; (d) The original creation date of the registration; (e) The expiration date of the registration; (f) The name and postal address of the SLD holder; (g) The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the SLD; (h) The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the SLD.

Id.

39. *Id.*

40. *Id.*

WHOIS.[41]

D. Use of Trademarks as Domain Names

Because products and services are best known by their trademark, it is common practice for trademark owners to incorporate their mark into the domain name of the company's home website. It is important for companies to include their mark in their domain name because it is by this trademark that consumers distinguish the products or services of one company from those of another.[42] Trademark rights are provided for by the United States Constitution, which states that "[t]he Congress shall have power . . . to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."[43]

The trademark rights afforded to an owner of a mark registered with the United States Patent and Trademark Office ("USPTO")[44] are much more extensive than common law trademark rights.[45] Pursuant to the Lanham Act,[46] individuals who register their mark secure, among other rights,[47] "the right to bring an action in federal court for trademark infringement," the right to "a possible basis to claim priority to an Internet domain name," and "prima facie evidence of . . . the registrant's exclusive right to use the mark in connection with the identified goods and services."[48]

The domain name registration process has created serious legal issues pertaining to trademarks.[49] Unlike the laws

41. *See generally WHOIS.Net: Domain-Based Research Services, at* http://www.WHOIS.net/ (last visited Sept. 17, 2004); *NetworkSolutions: WHOIS Search, at* http://www.networksolutions.com/en_US/WHOIS/index.jhtml (last visited Sept. 17, 2004).

42. Look, *supra* note 1, at 818.

43. U.S. CONST. art. I, § 8, cl. 8.

44. *See* U.S. Patent & Trademark Office, *Our Business: An Introduction to the USPTO, at* http://www.uspto.gov/web/menu/intro.html (last visited Sept. 17, 2004) (describing purpose of the USPTO and the services provided by the agency).

45. *See* BOUCHOUX, *supra* note 5, at 21 (noting that registration of a common law trademark is not necessary to acquire trademark rights). At common law, "trademark rights arise from use of a mark." *Id.*

46. 15 U.S.C. § 1051 (2000). *See also* BOUCHOUX, *supra* note 5, at 22 (stating that the Lanham Act is also known as the United States Trademark Act).

47. For a complete listing of the rights arising from federal registration of a copyright see United States Trademark Act of 1946, 15 U.S.C. § 1051 (detailing the rights trademark owners are granted by this Act). *See also* BOUCHOUX, *supra* note 5, at 21-22 (discussing trademark rights resulting from federal registration).

48. BOUCHOUX, *supra* note 5, at 22.

49. *See id.* at 110 (describing issues affecting trademark owners resulting from the popularity of the Internet).

regulating the registration of trademarks, the rules for registering a domain name do not include any procedure to ensure that a requested domain name is not infringing upon a previously registered domain name[50] or trademark.[51] As a result, not only is it easy, but it can also be very profitable for a registrant to register a domain name that includes a federally registered trademark to which the registrant has no rights.[52]

One can register domain names in violation of trademark laws in a number of ways and for a variety of purposes. One of the most prevalent and profitable ways that domain names are misused is when a person registers common misspellings of a well-known trademark, and then routes the traffic from the domain name to unrelated websites for a commission from the owner of the website to which the traffic is routed.[53] Another prevalent misuse of domain names arises when a person "trade[s] on the goodwill associated with" a well-known mark by registering a domain name that incorporates the mark.[54] Although it is

50. An example of infringing on a previously registered domain name is registering misspellings of domain names.

51. *See* Look, *supra* note 1, at 818-20 (listing the statutory bars to the registration of trademarks that are "confusingly similar" to a previously registered mark).

52. *Id.* at 818-21 (describing how the functional differences between trademarks and domain names cause conflicts to arise).

53. *See* Shields v. Zuccarini, 254 F.3d 476, 479-80 (3d Cir. 2001) (discussing a lawsuit in which an internet domain name wholesaler registered five variations, including "joescartoon.com," "joecarton.com," "joescartons.com," "joescartoons.com," and "cartoonjoe.com," of plaintiff's website and routed the traffic to his own website which trapped users in a succession of advertisements which had to be "clicked" before the user could exit). The advertisers paid the wholesaler "between ten and twenty-five cents" for every "click" on an advertisement. *Id.* at 480. *See also* Sports Auth. Mich., Inc. v. Haywood Jablome, Claim No. FA0209000124861 (Nat'l Arb. Forum Nov. 4, 2002) (Franklin, Arb.), *available at* http://www.arb-forum.com/domains/decisions/124861.htm (discussing a lawsuit in which defendant registered the domain name "wwwsportauthority.com" in violation of the Complainant's trademark and commercial website, "thesportsauthority.com"). The defendant directed the traffic from his domain name to the Complainant's home website and then signed up for the Complainant's affiliate program that paid a commission to a domain name holder who routes internet traffic to the home website of the Complainant. *Id.*

54. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 580 (N.D. Cal. 1999). *See also* H-D Michigan, Inc. v. Chad Morris, Claim No. FA0212000137094 (Nat'l. Arb. Forum Jan. 29, 2003) (Dorf, Arb.), *available at* http://www.arbforum.com/domains/decisions/137094.htm (discussing the lawsuit for trademark infringement by the trademark owner of "HARLEY" and "HARLEY DAVIDSON" against the registrant of the domain names "harleyleases.com," "harleyanniversary.com," "2003harleydavidson.com," "2003harley.com," "2004harley.com," and "2005harley.com" who attempted to sell the domain names for $300,000 on eBay); *Seescandy.com*, 185 F.R.D. at 575-76, 579 (discussing a lawsuit for trademark infringement by the trademark owner of "SEE'S," "SEE'S CANDIES," and "FAMOUS OLD TIME"

profitable for the infringer, routing traffic to unrelated websites can have an extremely negative impact on the goodwill associated with the trademark.[55]

In an effort to protect trademark owners from trademark infringement resulting from domain name registration, Congress enacted the AntiCybersquatting Consumer Protection Act ("ACPA")[56] and the Uniform Domain Name Dispute Resolution Policy ("UDRP").[57] Although the ACPA and UDRP provide trademark owners with greater power to enforce their rights in the on-line environment, the ability to identify and locate infringement offenders—especially repeat offenders—remains a major obstacle, preventing the adequate protection of trademarks on the Internet. This identification issue, trademark owners

---

against the registrant of the domain names "seescandy.com" and "seescandys.com," who indicated he was willing to sell the offending domain names to the trademark owner and offered evidence that the infringing domain names had actually confused customers); Am. Online, Inc. v. Huang, 106 F. Supp. 2d 848, 850 (E.D. Va. 2000) (discussing the lawsuit for trademark infringement by the trademark owner of "ICQ" against the registrants of the domain names "picq.com" and "picq.net" and "cicq.net"). *But see Strick Corp.*, 162 F. Supp. 2d at 375-76 (holding in a trademark infringement action that although the domain name "strick.com" incorporated a well known trademark, the registrant did not intend to "confuse or deceive Plaintiff's customers," and so the domain name did not infringe upon the trademark).

55. This is especially true if the user is routed to an unrelated pornographic website, which is common due to the fact that pornography websites often offer the highest commissions. Consider, for example, the backlash from angry parents that would occur if someone registered a misspelling of the "toysrus.com" domain name and routed it to a pornography or gambling website. *See Shady Sites, Do Lax Domain Name Rules Invite Scams?*, REDEYE, Sept. 5, 2003, at 44 [hereinafter *Shady Sites*] (stating a Miami man was charged with "using misspelled domain names to direct Web surfers to pornography sites").

56. Anticybersqatting Consumer Protection Act, Pub. L. No. 106-113, 113 Stat. 1501A-545 (1999) (codified in relevant part at 15 U.S.C. § 1125(d)).

> The purpose of the bill is to protect consumers and American businesses, to promote the growth of online commerce, and to provide clarity in the law for trademark owners by prohibiting the bad-faith and abusive registration of distinctive marks as Internet domain names with the intent to profit form the goodwill associated with such marks-a practice commonly referred to as "cybersquatting."

Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona, 330 F.3d 617, 624 (4th Cir. 2003).

57. ICANN, *Uniform Domain Name Dispute Resolution Policy*, *at* http://www.icann.org/udrp/udrp-policy-24oct99.htm (last visited Sept. 14, 2004). Pursuant to the UDRP, the registrant of a domain name must submit to a mandatory administrative proceeding if a third party complainant files a grievance with one of the four dispute resolution providers claiming that: (1) the registrant's domain name "is identical or confusingly similar to a trademark or service mark in which the complainant has rights"; (2) the domain name registrant has "no rights or legitimate interests in respect of the domain name"; and (3) the domain name "has been registered and is being used in bad faith."

argue, would be resolved if the information in the WHOIS was accurate. Of course, requiring a domain name registrant to provide accurate personal contact information on a publicly accessible database poses privacy rights issues of equal importance.

II. HISTORY OF PRIVACY AND TRADEMARK RIGHTS RELATING TO THE INTERNET

A. Privacy Guarantees of the First and Fourth Amendments

The privacy argument for not validating the personal information that is given by domain name registrants and then uploaded to the WHOIS—thereby making it possible for the registrant to remain anonymous—is based on the First Amendment's freedom of speech provision[58] and the Fourth Amendment's protection against unreasonable searches.[59] Specifically, some argue that the "free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously," and that the loss of anonymity "would have a significant chilling effect on Internet communications."[60] "While the U.S. Constitution does not expressly grant a general right to privacy, the U.S. Supreme Court has interpreted the U.S. Constitution as granting individuals a right to privacy that is incrementally derived from various constitutional guarantees," including "the First Amendment's protection of free speech and freedom of assembly" and "the Fourth Amendment's prohibition on unreasonable searches."[61] However,

58. U.S. CONST. amend. I.

59. U.S. CONST. amend. IV.

60. Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) (discussing the effect on speech that would result if the court allowed Internet users to be stripped of anonymity by enforcing the subpoena power granted by the broad rules of discovery). *See also* Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 304-05 (2001) (arguing "anonymity is an essential tool in protecting free speech and action on the Internet, even if accountability is marginally diminished").

61. Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution* 7 J. TECH. L. & POL'Y 123, 124 (2002). *See also* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (stating "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment"); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341-43 (1995) (stating that anonymous speech is a great tradition that is woven into the fabric of this nation's history). "[T]he interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure." *Id.* at 342. *Accord 2TheMart.com*, 140 F. Supp. 2d at 1097 (concluding that "the constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be

the U.S. Supreme Court has not yet spoken on the issue of how the right to privacy should be dealt with in the on-line context, "where greater degrees of anonymity are possible and where anonymity can more easily be exploited to illicit ends."[62]

B. Arguments in Favor of More Extensive Privacy Protection

The standard information provided as a result of a domain name query of the WHOIS database is the registrant's contact information, the contact information for the person or entity responsible for the technical aspects of the website associated with the specified domain name, and information pertaining to the creation and expiration date of the domain name.[63] The WHOIS limits personal information about the registrant to name, address, email, phone, and fax number.[64] Essentially, the database provides no more information about an individual or business than is available in a phone book. In and of itself, the information has a very limited effect on privacy expectations; however, this basic contact information, when taken in conjunction with the

---

carefully safeguarded"); *Seescandy.com*, 185 F.R.D. at 578 (stating that the "ability to speak one's mind" on the Internet "without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate"); Talley v. California, 362 U.S. 60, 65 (1960) (stating that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance"). *But see 2TheMart.com*, 140 F. Supp. 2d at 1093 (suggesting that the right to speak anonymously is not absolute).

62. Brenner, *supra* note 61, at 140.

63. For example, a "WHOIS" query of the domain name "kellyclarkson.com" at http://WHOIS.net (last visited Sept. 20, 2004) contains the following DNS data:

Domain name: kellyclarkson.com

Administrative [and Billing, Technical, Registrant] Contact:
Marc Hustant (marchustant@yahoo.com)
+39.0220480272
Fax: +39.0220480217
Via Ignazio Ribotti 28
Milano, IT 20124
IT

Status: Locked

Name Servers:
dns1.name-services.com
dns2.name-services.com
dns3.name-services.com
dns4.name-services.com
dns5.name-services.com

Creation date: 19 Jun 2002 11:19:28
Expiration date: 19 Jun 2006 11:19:28

64. *Id.*

corresponding website, provides such specific and comprehensive information about the registrant that it raises serious privacy and freedom of speech issues.[65]

The privacy issues that are central to the argument in favor of stronger privacy considerations pertaining to the WHOIS can be divided into three categories: mass solicitation, individual targeting, and the suppression of political and social discussion. The mass solicitation issue is based on the concern that companies will "harvest" contact information from the WHOIS and use that information for mass marketing purposes such as spam,[66] mass mailings, and telemarketing. The individual targeting category encompasses a wide variety of concerns about the use of information to target specific individuals for purposes such as identity theft and stalking.[67] The third category of concerns is based on the theory that anonymity promotes political and social debate and individual expression, because it provides the speaker with protection from retaliation.[68]

---

65. Consider, for example, this hypothetical. John Doe is a member of the Ku Klux Klan. He has been very active in the organization for twenty years, although he only participates in lawful demonstrations and he takes full advantage of his constitutional right to keep his identity secret. Not even his co-workers or his closest friends have any idea that he is a racist. When John meets new people that want to contact him, he tells them to use the phone book to contact him (he does not mind having his information available to the public in the phone book because it does not really tell anything about him). . In an effort to educate others about his racist viewpoints, John develops a website and registers a domain name (he realizes that the Internet reaches more people around the world than any other type of communication medium). As a result of his registering a domain name, his contact information is associated with his website, and ultimately his personal beliefs. Eventually, those people with whom he associates on a regular basis know that John is a racist and he is subject to many different types of retaliation. Ultimately, because he was unable to remain anonymous, John is forced to make a decision whether to terminate his participation in the Ku Klux Klan so that retaliation against him will stop or to continue exercising his constitutional rights at the expense of his prior relationships. Because he was unable to remain anonymous when he posted a website, his privacy was diminished and his ability to communicate his social views with others was diminished.

66. *See Trainer Statement*, *supra* note 38, at 11 (defining "spam" as "unsolicited, bulk mailings" via email).

67. *See* Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1005–06 (N.H. 2003) (describing a stalker's use of data collected electronically to plan and carry out the murder of his victim).

68. See *Reno*, 521 U.S. at 870 (holding that First Amendment protections extend to speech via the Internet because "[t]hrough the use of web pages, mail exploders, and newsgroups, [a person] can become a pamphleteer). *See also McIntyre*, 514 U.S. at 357 (explaining anonymity "exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from relation – and their ideas from suppression—at the hand of an intolerant society"). *See also* Roth v. United States, 354, U.S. 476, 484 (1957) (stating that political expression is entitled to the broadest protection "to assure the unfettered interchange of ideas for the bringing about

C. The Argument in Favor of Making Trademark Rights Paramount to Privacy Rights when Conflicts Arise

In contrast to the broad range of issues that are important to the privacy advocates, the argument of trademark owners is much narrower, but no less important. The major concern of trademark owners is that they have a means to locate and enforce their trademark rights against parties who register domain names that infringe on their mark.[69] In fact, it has been suggested that "[u]ntil another method of identifying those behind certain web sites is created, WHOIS remains the only tool for companies looking to protect their intellectual property rights on the Internet."[70]

D. Administration of the WHOIS and Resulting Conflicts

1. Balancing test approach

The most common approach taken by courts when addressing an issue that pits trademark rights against privacy rights is to use a balancing test.[71] The downside to a balancing test is that controlling precedent is rarely applied consistently due to the low probability that the material facts of later cases will be substantially similar to those of prior cases. Although it would be difficult to apply a different type of test to such cases under the current administration of the WHOIS, a change in the approach of

---

of political and social changes desired by the people"). *See also Talley*, 362 U.S. at 64 (stating "[a]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind").

69. *See Trainer Statement*, *supra* note 38, at 8 (explaining that trademark owners use the WHOIS information in a variety of ways, including (1) contacting a website operator directly, demanding the unlawful activities cease; (2) mapping infringers activities in order to determine patterns of behavior which can be used against the infringer in subsequent criminal or civil enforcement proceedings; and (3) helping prove the bad faith of a cybersquatter).

70. *Id.*

71. *See 2TheMart.com*, 140 F. Supp. 2d at 1093 (discussing the best way to resolve a conflict between two competing rights). The court explained that in cases in which the plaintiff requested the court issue a subpoena to permit the acquisition of the identity of persons who have exercised their First Amendment right to speak anonymously, there was "little in the way of persuasive authority to assist," but that "courts that have addressed related issues have used balancing tests to decide when to protect an individual's First Amendment rights." *Id.* at 1094. *See also Seescandy.com*, 185 F.R.D. at 578 (discussing an individual's right to "participate in on-line forums anonymously or pseudonymously" versus allowing "discovery to uncover the identity of a defendant" so that they might be properly served and subject to the jurisdiction of the court).

the administration of the database would be extremely beneficial to the protection of the rights of the parties on both sides of the trademark rights versus privacy rights debate. In addition, it would result in a much greater degree of predictability as to the outcome of such disputes, and it would enable the decisions of the court to be more efficiently and effectively enforced.

2. Terms of use agreements

It is a standard requirement that a person who intends to access or query the WHOIS must first agree to a terms of use agreement and notice[72] ("query agreement"). This binds the user to use the data obtained from the database for lawful purposes only, and not to use the information for the purpose of facilitating mass, unsolicited advertising. Violation of this agreement gives the registrar the right to terminate the user's access to the database.[73]

Similarly, the standard service agreement between the registrant and the registrar[74] ("registration agreement"), a prerequisite to registering a domain name, requires that the registrant provide true, complete, and accurate information.[75]

---

72. The standard agreement that is binding on a party who submits a WHOIS query can be found at http://networksolutions.com/en_US/WHOIS/index.jhtml (last visited Sept. 24, 2004). Standard terms are:

> You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes.... [The] database is provided for information purposes only, and to assist persons in obtaining information about or related to a domain name registration.... By submitting a WHOIS query, you agree ... that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes.... The compilation, repackaging, dissemination or other use of this data is expressly prohibited.... [The registrar] reserves the right to terminate your access to the WHOIS database at its sole discretion ... for excessive querying of the WHOIS database or for failure to otherwise abide by these terms.

Id.

73. *Id.*

74. A typical agreement that is binding on a party who registers a domain name with any DNS registrar can be found at http://www.register.com/service-agreement.cgi?cmp=IL10682 (last visited Sept. 24, 2004). Standard terms of a registrant/registrar contract require the registrar to warrant that: (a) the information provided is "complete and accurate"; (b) "registration of the domain name will not infringe upon or otherwise violate the rights of any third party"; (c) the domain name is not being registered for an "unlawful purpose"; and (d) the domain name will not be used in violation of "any applicable laws or regulations." *Id.*

75. *See id.* (stating a registrant of a domain name is obligated to "provide and keep current" (a) his full name or the authorized contact person if

Violation of this agreement gives the registrar the right to terminate the registrant's use of the domain name.[76]

3. *Current problems with WHOIS administration*

The WHOIS's current failure to enforce the registration and query agreements, combined with the fact that user information is not a required entry when a search of the WHOIS is performed, results in a system that is completely lacking accountability.[77] Without accountability, there exists no check on the misuse of the system or on the violation of both privacy and trademark rights.[78] The pervasiveness of the problem is readily apparent by the fact that over 4,000 disputes[79] involving over 7,000 domain names have been arbitrated under the UDRP.[80]

Furthermore, a system lacking accountability presents due process problems. Because one cannot serve notice of a lawsuit on an anonymous wrongdoer, there can technically be no lawsuit brought against such a violator.[81]

---

registrant is an organization, corporation or association; (b) postal address; (c) e-mail address; (d) telephone and fax number; (e) the domain name being registered; and (f) the "name, postal address, e-mail address, [and] voice telephone number . . . for the administrative contact, technical contact and billing contact for the domain name registration")

76. *See id.*

> [Registrants] acknowledge and agree that Register.com may suspend, cancel, transfer or modify your use of the Services at any time, for any reason, in Register.com's sole discretion . . . if you materially breach this Agreement . . . and do not cure such breach within five (5) calendar days . . . [or] if you use the domain name registered to you to send unsolicited commercial advertisements . . . or . . . if you use the domain name in connection with unlawful activity.

Id.

77. *See* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 146 (1996) (arguing that a precondition for all enforcement is the absence of anonymity).

78. *See McIntyre*, 514 U.S. at 385 (Scalia, J., dissenting) (arguing the "very purpose" of anonymity is the facilitation of wrongs by "eliminating accountability").

79. *See* Suzanna Sherry, *Haste Makes Waste: Congress and the Common Law in Cyberspace*, 55 VAND. L. REV. 309, 355 (2002) (analyzing the effectiveness of the provisions of the ACPA).

80. *See Trainer Statement*, *supra* note 38, at 5 (arguing the registration of domain names that infringe on trademarks is a major problem and without accurate WHOIS information, there is very little that trademark owners can do to protect themselves).

81. *See* Mullane v. Cent. Hanover Bank & Trust Co., 339 U.S. 306, 314 (1950) (requiring "notice reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections"). *But cf.* Lehr v. Robertson, 463 U.S. 248, 264 (1983) (holding that the failure to provide actual notice to a domain name registrant who provides incorrect information or fails to keep registration information current, does not raise a due process problem because

Although Congress, through the passage of the ACPA,[82] has attempted to resolve the "due process problem" of bringing a lawsuit against an unknown defendant in trademark infringement cases pertaining to the misuse of a domain name,[83] enforcement of a judgment resulting from such a suit is at best problematic and at worst impossible. A major problem with enforcing a judgment from a case brought under the in rem provision of the ACPA is that anonymous defendants who are non-U.S. residents are technically beyond the jurisdiction of a United States court.[84] Although decisions by the courts in cases such as these have been enforced, they have generated a substantial amount of international controversy.[85] Some suggest that continued extraterritorial application of the United States' trademark laws could result in the segmentation[86] of the domain system.[87] Segmentation would drastically decrease the utility of the DNS.[88]

"the right to receive notice was completely within appellant's control").

82. 15 U.S.C. § 1125(d)(2)(A).

83. *See id.* (authorizing an in rem civil action against domain name registrants that cannot be located or subjected to the jurisdiction of a United States court). The purpose of the in rem provision was to address the problem faced by trademark owners when "cybersquatters register domain names under aliases or otherwise provide false information in their registration applications in order to avoid identification and service of process by the mark owner." H.R. REP. NO. 106-412, at 14 (1999). Under the ACPA, a trademark owner who has a claim against the anonymous registrant of a domain may sue the domain name instead of the registrant "in cases where the plaintiff has in good faith exhausted traditional avenues for identifying a civil defendant pre-service." *Seescandy.com*, 185 F.R.D. at 578. *See also* Struve & Wagner, *supra* note 3, at 998-1007 (explaining in detail the purpose of the ACPA in rem provision and the requirements that a plaintiff must meet before this provision can be effectuated).

84. *See* Struve & Wagner, *supra note 3,* at 1000-19 (examining the constitutionality of in rem and in personam jurisdiction in cases in which the defendant is either anonymous or is beyond the jurisdiction of a United States court). It has been suggested that in cases of foreign cybersquatting ("where a non U.S. resident cybersquats on a domain name that infringes upon a U.S. trademark") section 1125(d)(2)(A)(ii)(I) will either be not applicable or unconstitutional. *Id.* at 998.

85. *See id.* at 1026 (suggesting prescriptive jurisdiction by U.S. courts will likely generate a "substantial international controversy"). *See also* Joseph P. Griffin, *United States Antitrust Laws and Transnational Business Transactions: An Introduction*, 21 INT'L LAW. 307, 308-09 (1987) (explaining other nations have passed more than fifteen "blocking statutes" in response to the "extraterritorial application of the U.S. antitrust laws"); Thomas C. Fischer, *Case Two: Extraterritorial Application of United States Law Against United States and Alien Defendants (Sherman Act)*, 29 NEW ENG. L. REV. 577, 585-86 (1995).

86. Segmentation arises when data on one of the servers that is part of the DNS "are either in conflict or do not accurately reflect the content" of other servers in the system. Struve & Wagner, *supra* note 3, at 1032.

87. *Id.* at 1031-32.

88. *Id. at* 1032.

E. Changes Necessary to Improve the Utility of the WHOIS

Obviously, the importance of the rights at issue necessitates that changes be made to the administration of the WHOIS and the DNS registration process in order to more adequately protect both trademark and privacy rights. Instead of relying on Congress to pass more legislation in an effort to resolve these issues, the Internet community should take the initiative and institute changes.

The entities in charge of domain name registrations and WHOIS queries must start enforcing the contracts that are already in place.[89] Specifically, if a registrant does not provide complete and accurate information, or repeatedly registers domain names that violate the rights of another, the registrar should enforce the terms of the registration agreement and "suspend, cancel, transfer, or modify" the offender's domain name registration.[90] Similarly, administrators of the WHOIS must enforce the query agreement so that persons who query the WHOIS for unlawful purposes have their access to the WHOIS terminated.[91] Likewise, the registries must start denying top-level domain name registration to any registrar that repeatedly allows registrants to violate the terms of the registration and query agreements. Such action by a registry, even if it violates a contractual provision, would arguably be upheld by the courts in a judicial proceeding because "the interest in vindicating congressionally provided trademark rights trumps contract."[92]

The administrators of the WHOIS, to more efficiently and effectively protect privacy and trademark owners' rights, must implement some type of identification requirement of people

---

89. On September 4, 2003, the House Committee on the Judiciary, Subcommittee on Courts, the Internet, and Intellectual Property, held a hearing on whether an extension of ICANN's arrangement with the Commerce Department would be proper. A central issue of Chairman Lamar Smith's opening statement was the lack of enforcement of existing contractual agreements. He stated that there was "an astonishing lack of enforcement of these contractual terms" and that the specific failure to make sure that WHOIS data is accurate "undermine[s] the very authority, stability, sustainability [the] Commerce [Department] purports to want to ensure for ICANN." *Internet Domain Name Fraud – the U.S. Government's Role in Ensuring Public Access to Accurate WHOIS Data: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the House Comm. on the Judiciary*, 108th Cong. 2 (2003) (statement of Lamar Smith, Chairman).

90. http://www.register.com/service-agreement.cgi?cmp=IL10682 (last visited Sept. 24, 2004).

91. *See* http://www.networksolutions.com/en_US/legal/static-service-agreement.jhtml (last visited Sept. 24, 2004) (stipulating that querying the WHOIS for an unlawful purpose will result in the termination of access to the database).

92. *GlobalSantaFe*, 250 F. Supp. 2d at 623.

accessing the WHOIS. A simple and inexpensive method of achieving this type of accountability is to password-protect the database. A user attempting to access the database would be required to provide an e-mail address to which a password would automatically and immediately be sent. A third party organization would store the performed search and the information pertaining to the address provided by the user. This system would eliminate conflicts of interest that currently arise as a result of competition between registrars, and between registrars and registrants.[93] The third-party organization would be responsible for storing and protecting the query information, and would use it only to satisfy a subpoena in lawsuits in which the court determines the information to be material.

III. MAKING ACCOUNTABILITY AN INTEGRAL ASPECT OF THE WHOIS

The requirement of accountability in the WHOIS will provide substantial benefits to every individual or entity that uses the database for legitimate purposes, while imposing minimal negative effects on legitimate users. Trademark owners will benefit by having a reliable source that they can use to efficiently and effectively protect their marks. Personal information, although required to be true and accurate, will be protected because parties intending to use the information for illegal purposes will not be able to hide behind a veil of anonymity. The law-abiding consumer will benefit by being able to obtain accurate information that can be used to contact the domain name holder.

---

93. The most likely conflict of interest that could arise if there was not any third party is that, in the case of disputes involving the WHOIS, registrars would be responsible for turning over information that in many cases would be adverse to the interests of the users utilizing their website. Most likely, in such a situation, the registrants would resist providing information in order to be perceived as a company that was interested in protecting its customers. Similarly, the best customers of registrars, those who registered large quantities of domain names, would predictably be most inclined to do business with the registrars that were least cooperative in providing query information. Thus, the goal of gaining customers and earning a profit would motivate registrars to be uncooperative and to do everything possible to preserve a user's anonymity. *See Shady Cites*, supra note 55 (citing Harvard University researcher Ben Edelman, who suggested that it is often "in the registrar's interest to turn a blind eye to [WHOIS] entries to attract porn-site operators, who register thousands of domain names at a time"). *See also* Julie Hilden, *Why Anonymous Internet Speakers Can't Count on ISP's to Protect Them, at* http://writ.news.findlaw.com/hilden/20010101.html (Jan. 1, 2001) (acknowledging that customers may go elsewhere if the ISP does not protect the anonymity of its customers' speech, but that protecting anonymity is not crucial to the ISP as it is to a newspaper).

A. Benefits to Trademark Owners

Requiring accountability in the WHOIS will substantially benefit trademark owners. Unlike the current system, which makes violation of a trademark easy and the evasion of restitution or punishment even easier,[94] the proposed system will give an advantage to the trademark owner. Under the proposed system, trademark owners will be able to more efficiently and effectively serve process on violators because they will have more reliable information about the location of the violator. They will also be able to establish patterns of illegal conduct by analyzing WHOIS search information,[95] and enforce judgments more efficiently. The only substantial negative effect of the proposed system on trademark holders is that the implementation of password protection will make searches of the WHOIS more burdensome and time consuming. However, simple enhancements could be added to the system to negate this inconvenience. Overall, the proposed system will be very favorable to trademark owners.

B. Effects of Accountability on Privacy Rights

The effect of making accountability an aspect of the WHOIS would benefit privacy rights as much as it would trademark rights. In fact, one can argue that the proposed method of administration of the database would provide more protection to privacy than is currently provided. This argument is based on the fact that inherent to a process providing accountability is the elimination of absolute anonymity. Eliminating absolute anonymity will reduce crimes against privacy rights, and will ultimately be more favorable to privacy rights than a system in which anonymity were allowed to persist. This theory is best explained by an analysis of the specific issues with which privacy advocates are most concerned: mass solicitation, individual targeting, and loss of political and social discussion.

1. Privacy from mass solicitation

Requiring the WHOIS to reflect accurate information will have very little, if any, adverse affect on privacy rights as it

94. *See Seescandy.com*, 185 F.R.D. at 577 (describing the difficulty that domain name owners encounter in trying to enforce their trademarks against a domain name registrant who uses false information when registering a domain name). The *Seescandy.com* court recognized that the rise of the Internet has enabled tortfeasors to act pseudonymously or anonymously resulting in the inability of injured parties to discover the identity of the tortfeasor. *Id.* at 578.

95. *See* Elana Broitman, *ICANN: What is Whois?*, *at* http://www.whois.sc/news/2003-06/icann-whois.html (June 19, 2003) (explaining the WHOIS is important to IP owners for use in determining if "a particular registrant has developed a pattern of cybersquatting activities").

pertains to mass solicitation. The Internet community generally recognizes that it is necessary to prevent the use of the WHOIS for data harvesting and spamming purposes.[96] Although there are technical[97] and legal safeguards already in place to prevent the use of the WHOIS for these purposes,[98] password protection of the WHOIS will add a superior level of privacy protection to these safeguards for several reasons. First, it will be easy for WHOIS administrators to identify a person mining the database because such a person will need to make an unusually large number of requests for passwords.[99] Second, if a spammer attempts to evade detection by having WHOIS send passwords to multiple e-mail addresses, the mining will quickly become cost prohibitive.[100] Finally, the proposed system could aid law enforcement officials in tracking down and accumulating evidence to be used against spammers. Law enforcement will benefit because in order to obtain passwords, the spammers would have to set up an e-mail account, which usually requires a payment of money and a verification of identity. This would leave a trail for law enforcement officials to follow back to the violator.

2. Privacy from individual targeting

While mass solicitation can be prevented by charging the "gatherer" a nominal fee for every piece of data collected,[101]

96. *See Do Not Spam List Nears Final OK*, REDEYE, Nov. 26, 2003, at 4 (discussing a bill expected to be signed into law which would bar the "harvesting of addresses from Web sites" and would be targeted at curbing spam, "which now makes up about half of all e-mail").

97. *See WHOIS.Net: Domain-Based Research Services*, *at* http://www.WHOIS.net/ (last visited Sept. 24, 2004) (explaining how using a code embedded in an image that cannot be read by a machine prevents automated access to the information in the WHOIS). *See also WHOIS Lookup*, *at* http://www.register.com/whois-results.cgi?domain=v92.com&SRC= (last visited Dec. 6, 2004) (requiring a code to be entered before gaining access to the WHOIS, and explaining the "code is an image that cannot be read by a machine" and "[i]t prevents automated programs from requesting access to WHOIS information").

98. *See NetworkSolutions Enhanced Whois Directory*, *at* http://www.networksolutions.com/en_US/Whois/index.jhtml (last visited Sept. 24, 2004) (requiring the person implementing the WHOIS query to agree to terms of use which prohibits the use of "high volume, automated, electronic processes" to gather information from the database). Violation of this agreement can result in the termination of access to the database. *Id.*

99. *See Re: [ga] Privacy and Whois databases*, *at* http://www.dnso.org/clubpublic/ga/Archives/msg01157.html (last visited Sept. 24, 2004) (proposing changes to the administration of WHOIS and discussing the possible results of such changes).

100. *See id.* (suggesting spamming becomes prohibitively expensive when the spammer must spend money to circumvent privacy safeguards).

101. Nominal costs quickly become a major obstacle to profitability because of the huge amounts of information that must be gathered.

individual targeting is not affected by nominal costs, and the results of such targeting can be deadly.[102] At first it might seem that a proposal requiring the WHOIS to be accurate is unreasonable because it could aid individual targeting, but in fact the proposed system would deter violent crimes.

Those concerned with privacy argue that a major benefit of being able to post fictitious information on the WHOIS is that it protects the registrant from being the target of identity theft, harassment, and other crimes. In reality, however, not only is there little evidence that the WHOIS is being used for this purpose, but there are comparable alternative sources, such as private investigators or government websites,[103] from which the same type of information can be obtained. In addition, there are proven methods, such as contracting with a third party to be the registrant and technical contact of a domain name,[104] which allow an individual to satisfy the proposed WHOIS accuracy requirement and at the same time remain "pseudo-anonymous."[105] Furthermore, the proposed requirement of password-protection for the WHOIS would, in theory, discourage a user from using the WHOIS for illegal purposes, because the user would be on notice that his queries were being recorded. The fear that this record could be used as evidence against him if he used the information for illegal purposes would act as a deterrent.[106]

3. Privacy rights important to social and political discussion

The most controversial aspect of limiting anonymity at the expense of accountability is the possible chilling effect it could

---

102. *See Remsburg*, 816 A.2d at 1005–06 (describing a murder that was carried out through the use of personal data about the victim that was obtained through the Internet).

103. Personal information about the executives of a corporation or LLC can be obtained from Secretary of State websites such as the website for the Illinois Secretary of State, *at* http://www.cyberdriveillinois.com/departments/business_services/corporation_search/home.html (last visited Dec. 4, 2004).

104. For two examples of ways in which domain name owners use third parties in order to protect personal contact information, do a WHOIS search of "jenniferlopez.com" and "schaadfamilyalmonds.com" *at* http://www.networksolutions.com/en_US/whois/index.jhtml.

105. For lack of a better term, the author intends "pseudo-anonymous" to mean anonymous as it pertains to the WHOIS/Internet as opposed to absolute anonymity.

106. *See, e.g.*, postings of Srikanth Narra, Snarra@talus.net, and J. Baptista, bapt.stu@pccf.net, to Peter Veeck, Veeck@tetoma.net, *at* http://www.dnso.org/clubpublic/ga/Archives/msg01157.html (last visited Sept. 24, 2004) which suggests the WHOIS could be programmed to automatically send an e-mail to the owner of a domain name every time the domain name was queried. *See also* Elana Broitman, *ICANN: What is Whois?*, *at* http://www.whois.sc/news/2003-06/icann-whois.html (last visited Sept. 24, 2004) (suggesting domain name registrants could request from a registrar "a 'credit report' of who asked for their data, when, and for what purpose").

have on political and social discussion.[107] However, because there are a limited number of websites that are within the scope of this argument,[108] and consequently a limited amount of speech that would be affected, the proposed changes would most likely pass a constitutional analysis pertaining to freedom of speech and privacy rights. This is especially true considering that there are many alternatives available on the Internet to registering a domain name, such as using "chat rooms" which allow an individual to discuss political and social issues anonymously.[109] In addition, the proposed changes would still allow a political or social activist who uses a website as his medium a degree of anonymity comparable to that which could be found in the real world.[110] Complete anonymity is virtually impossible in the real world, and there has yet to be a court decision or legislation that grants an on-line user the right to a greater degree of anonymity than can be achieved in the real world. Therefore, until there is a shift in public policy that results in a need for political and social activists to enjoy a greater amount of anonymity on-line than can be found in the non-digital world, absolute anonymity must give way to accountability.

---

107. As discussed previously in this Comment, "[w]hen speech touches on matters of public political life . . . and advocacy of controversial points of view, such speech has been described as the 'core' or 'essence' of the First Amendment." *2TheMart.com*, 140 F. Supp. 2d at 1092-93. But "the right to speak anonymously is . . . not absolute." *Id.* at 1093.

108. Assuming that most websites are commercial and most political and social discussion takes place in chat rooms, which would not be affected by the WHOIS changes, it is very probable that the number of political websites adversely affected by the proposed WHOIS changes would be minimal. However, it does not really matter if this assumption is correct because any speech that is affected, due to a decrease in anonymity, will arguably only be affected to a degree that would bring it back in line with the amount of anonymity that is possible in the "real-world."

109. *See* Thomas C. Greene, *Do-It-Yourself Internet Anonymity*, *at* http://www.theregister.co.uk/content/55/22831.html (last visited Sept. 24, 2004) (discussing techniques to utilize in order to participate anonymously on the Internet). For information about services that provide a user with complete anonymity for web-surfing see *Free Anonymous Web Surfing* at http://www.the-cloak.com/anonymous-surfing-home.html (last visited Sept. 24, 2004), and http://ultimate-anonymity.com/main.html (last visited Sept. 24, 2004), which provides users a way to surf the web with "ultimate anonymity."

110. Absolute anonymity is arguably impossible to obtain in the real world. Consider a Ku Klux Klan member: Although his identity as a Klansman might be concealed from the public, it is probable that at least one other person knows of his affiliation with the organization or someone participated in his purchasing or making of his "outfit". Either way, the degree of anonymity is no greater than if a person made a political website, and then contracted with someone to register the website and not release his identity.

CONCLUSION

The domain name registration process and the administration of the WHOIS must change in order to balance the scales of justice as they pertain to trademark rights and privacy rights. As it currently stands, the ability to remain absolutely anonymous on the Internet enables individuals to commit crimes and act illegally in ways that would not be possible with "real world anonymity." The changes suggested in this Comment would provide trademark owners with the tools necessary to enforce their constitutionally protected rights, and at the same time protect the users' constitutionally guaranteed right to privacy.