Boston College Law Review

Volume 49
Issue 1 *Number 1*

Article 2

1-1-2008

Who Owns "Hillary.com"? Political Speech and the First Amendment in Cyberspace

Jacqueline D. Lipton

WHO OWNS "HILLARY.COM"? POLITICAL SPEECH AND THE FIRST AMENDMENT IN CYBERSPACE

JACQUELINE D. LIPTON*

Abstract: In the lead-up to the next presidential election, it will be important for candidates both to maintain an online presence and to exercise control over bad faith uses of domain names and web content related to their campaigns. What are the legal implications for the domain name system? This Article examines the large gaps and inconsistencies in current domain name law and policy as to domain name use in the political context. Current domain name policy focuses on protecting trademark uses of domain names against bad faith commercial "cybersquatters." It does not deal with protecting important uses of domain names as part of the political process. This Article identifies the current problems with Internet domain name policy in the political context and makes recommendations for developing clearer guidelines for uses of political domain names. In so doing, it creates a new categorization system for different problems confronting the political process in cyberspace, including: (a) socially and economically wasteful political "cybersquatting"; (b) political "cyberfraud," which might involve conduct such as registering a politician's name as a domain name to promulgate a misleading message about the politician; and (c) competition between politicians' names and competing trademark interests.

INTRODUCTION

Who owns "hillary.com"? Or "obama.com"? Or "giuliani.com"? How important might some of these names be in the lead-up to the next presidential election? If history is any guide, they could be extremely important, and valuable—as John Kerry found out the hard way after naming John Edwards as his running mate in 2004.[1] The "kerryedwards.com"

* Professor, Codirector, Center for Law, Technology, and the Arts, Associate Director, Frederick K. Cox International Law Center, Case Western Reserve University School of Law, 11075 East Boulevard, Cleveland, Ohio 44106, USA. Email: Jacqueline.Lipton@case.edu, Fax: (216) 368-2086. The author would like to thank Professors Margreth Barrett, Robert Denicola, and Mark Janis for insightful comments on earlier iterations of this project, as well as Professor Olufunmilayo Arewa for commenting on an earlier draft of this Article. All mistakes and omissions are my own.

[1] *See Nobody Wants Kerryedwards.com*, NETWORK WORLD, Aug. 3, 2004, http://www.networkworld.com/weblogs/layer8/005859.html (discussing attempt by Mr. Kerry Edwards of Indianapolis to auction the domain name kerryedwards.com to the highest bidder during

domain name was already registered to a Mr. Kerry Edwards, who attempted to auction it to the highest bidder throughout the course of the 2004 presidential election.[2] These issues are almost certain to arise again in the 2008 election. For example, Senator Hillary Clinton now owns "hillaryclinton.com," but the more generic "hillary.com" is registered to a software firm, Hillary Software, Inc.[3] What about "hillary2008.com"? It is registered to someone outside the Clinton campaign and currently purports to be "The Completely Unofficial Blog for Hillary's Brain."[4]

Internet domain names in the political context serve important purposes in identifying political websites to the public; these sites are becoming increasingly critical both to fundraise and to disseminate information about relevant policy issues.[5] An Internet presence is now invaluable to a politician.[6] The Internet can be used to reach an audience on a scale never before possible for a fraction of the cost of other media conduits.[7] In some respects, this potentially levels the playing

---

the course of the 2004 presidential election); *No Sale for KerryEdwards.com*, MARKETWATCH, Aug. 2, 2004, http://www.marketwatch.com/news/story/no-sale-kerryedwardscom/story.aspx?guid=%7BA230A724%2D4E01%2D4B66%2D95B9%2D76D9B305F681%7D [hereinafter *No Sale*]; *Web Address Fails to Attract $150,000 Minimum Bid*, USATODAY.COM, Aug. 2, 2004, http://www.usatoday.com/tech/webguide/internetlife/2004-08-02-kerryedwards_x.htm [hereinafter *Web Address Fails*]; *see also* PEW INTERNET & AM. LIFE PROJECT, THE INTERNET AND CAMPAIGN 2004, at 12 (2005), *available at* http://www.pewinternet.org/pdfs/PIP_2004_Campaign.pdf (finding about a quarter of Internet users visited at least one presidential campaign or national political party website in 2004).

[2] *No Sale*, *supra* note 1; *Web Address Fails*, *supra* note 1; *see Nobody Wants Kerryedwards.com*, *supra* note 1.

[3] *See* Hillary Software, Inc., http://www.hillary.com (last visited Oct. 28, 2007).

[4] *See* Hillary 2008, The Completely Unofficial Blog for Hillary's Brain, http://www.hillary2008.com (last visited Oct. 28, 2007).

[5] *See, e.g.*, PEW INTERNET & AM. LIFE PROJECT, *supra* note 1, at 1, 12–14 (discussing candidate fundraising online, and voters' visits to campaign websites); Glen Justice, *Kerry Kept Money Coming with Internet as His A.T.M.*, N.Y. TIMES, Nov. 6, 2004, at A10 (reporting online fundraising success of John Kerry's 2004 presidential campaign and noting increase in online campaign fundraising since 2000).

[6] *See, e.g.*, PEW INTERNET & AM. LIFE PROJECT, *supra* note 1, at iv (reporting immense growth in Internet use to obtain political information); Caroline J. Tolbert & Ramona S. McNeal, *Unraveling the Effects of the Internet on Political Participation?*, 56 POL. RES. Q. 175, 177 (2003) (noting that candidate websites during the 2000 U.S. presidential election included position papers, rebuttals of other candidates' statements, and fundraising appeals); Lisa Napoli, *Like Online Dating, with a Political Spin*, N.Y. TIMES, Mar. 13, 2003, at G1 (discussing activities of the Howard Dean campaign at "www.deanforamerica.com" and the use of the Internet as a key part of the campaign's strategy).

[7] *See* Fed. Election Comm'n, Internet Communications, 71 Fed. Reg. 18589, 18589–91 (proposed Apr. 12, 2006) (distinguishing Internet from print and other media as lower cost and nearly unlimited).

field for politicians and political commentators alike regardless of their fundraising abilities.[8]

An Internet presence with an easy-to-guess and easy-to-recognize domain name can, however, cause problems for politicians.[9] Many of the problems stem from the fact that the current Internet domain name regulation system is largely premised on protecting commercial trademark interests in domain names,[10] not on protecting political interests.[11] There are significant gaps in the law when it comes to the use of domain names in politics.[12] Particularly during a political campaign, it is important that those wishing to use available media to discuss candidates and their views should be able to do so in the least socially misleading and least economically wasteful way possible. There are no clear rules about how domain names, particularly those corresponding to politicians' names, may be used legitimately in the political process.[13]

The current domain name regulation system is focused on preventing trademark-based cybersquatting.[14] "Cybersquatting" in this context has been described as speculatively purchasing a domain name with the intention of selling it for a profit—usually with respect

---

[8] *See, e.g.*, Napoli, *supra* note 6 ("For candidates like Dr. Dean, who do not have large coffers or high national name recognition, the Web is an indispensable grass-roots medium.").

[9] *See* Steve Friess, *As Candidates Mull '08, Web Sites Are Already Running*, N.Y. TIMES, Nov. 18, 2006, at A15 (discussing candidate-name-based domain names registered by private individuals years before the elections).

[10] Jacqueline Lipton, *Beyond Cybersquatting: Taking Domain Names Past Trademark Policy*, 40 WAKE FOREST L. REV. 1361, 1363 (2005). ("[T]he current dispute resolution mechanisms [for domain name disputes] are focused on the protection of commercial trademark interests, often to the detriment of other socially important interests that may inhere in a given domain name.").

[11] *Id.* at 1425–31 (discussing the gaps in current regulations in the political context).

[12] *See infra* notes 119, 322 and accompanying text (discussing absence of particular rules for politics in federal legislation); *see also* Denise Pereira, Note, *Chapter 277: California's Solution to Cyberfraud in the Political Arena*, 35 MCGEORGE L. REV. 399, 401–02 (2004) (noting previous legislative version of the Federal Anticybersquatting Consumer Protection Act had included political domain name regulation, but that the provisions were rejected).

[13] *See* Friess, *supra* note 9 ("Experts are split on whether a campaign can force a registrant to give up a domain name without compensation on the ground that it bears the candidate's name.").

[14] *See* 15 U.S.C.A. §§ 1125(d), 1129 (West 1998 & Supp. 2007); Internet Corp. for Assigned Names & Numbers ("ICANN"), Uniform Name Dispute Resolution Policy ("UDRP") (Oct. 24, 1999), http://www.icann.org/udrp/udrp-policy-24oct99.htm [hereinafter UDRP] (establishing private domain name dispute policy for international arbitration).

to a well-known name corresponding to a trademark.[15] Application of current laws to prevent misleading or wasteful registrations and uses of *political* domain names is limited in two ways. The first is that current laws mainly protect trademarked and, therefore, *trademarkable* political domain names,[16] and the second is that the present legal regime only protects those names against bad faith cybersquatting.[17] These are serious limitations. Many politicians' names will not be federally registrable as trademarks, at least in the political, as opposed to commercial, context.[18] Many politicians' names may not even attain a common law trademark status if used in a purely political, as opposed to a commercial, context.[19] Further, much of the abusive conduct that arises in an electoral context involves misleading *content* on a political website associated with a particular domain name, rather than an attempt to sell the domain name for a profit.[20]

This Article makes two important contributions to the debate on facilitating effective political speech in cyberspace. The first is to cre-

---

[15] *See* John D. Mercer, Note, *Cybersquatting: Blackmail on the Information Superhighway*, 6 B.U. J. SCI. & TECH. L. 11, ¶ 4 (2000) ("[C]ybersquatting occurs when an individual or corporation registers a domain name that is spelled the same as a pre-existing trademark, and demands money from the trademark owner before the registrant will release the domain name."); *see also* 15 U.S.C.A. § 1125(d); Ira Nathenson, Comment, *Showdown at the Domain Name Corral: Property Rights and Personal Jurisdiction over Squatters, Poachers and Other Parasites*, 58 U. PITT. L. REV. 911, 925–26 (1997); Dictionary.com, http://dictionary.reference.com/browse/cybersquatting (last visited Oct. 13, 2007) (defining cybersquatting as "the registration of a commercially valuable Internet domain name, as a trademark, with the intention of selling it or profiting from its use").

[16] *See* 15 U.S.C.A. § 1125(d).

[17] *See id.*

[18] Generally, personal names are not registrable as trademarks. *See* Trademark (Lanham) Act of 1946, 15 U.S.C. § 1052(c) (2000); *see also* ANNE GILSON LALONDE ET AL., GILSON ON TRADEMARKS § 2.03[4][d] (2007) (stating personal name must acquire secondary meaning to be protectable). Although a personal name may be registrable on the federal trademark register with the consent of the person whose name it is, in order to *maintain* registration, the name must function as a trademark; in other words, it must be able to distinguish the goods of the applicant for registration from the goods of others. 15 U.S.C.A. § 1052 (West 1997 & Supp. 2007). If it serves purely political purposes and does not distinguish goods or services in commerce, it is unlikely to retain its registration. *See id.* Thus, some politicians could choose to register their names as trademarks in order to protect them from unauthorized use, but the registration would only be valid in the commercial trademark context and not necessarily in the noncommercial speech or political context. *See id.*

[19] *See* Friends of Kathleen Kennedy Townsend v. Birt, No. D2002-0451, ¶¶ 4(b), 5 (WIPO July 31, 2002), http://www.wipo.int/amc/en/domains/decisions/word/2002/d2002-0451.doc (acknowledging prior finding that protection of a politician's name was not protectable under the UDRP because not commercially exploited, and stating her committee had not shown the mark was registrable).

[20] *See* Friess, *supra* note 9.

ate a novel categorization scheme for the various types of domain name registrations that may cause problems for politicians.[21] The development of this categorization scheme is essential in the political context.[22] In fact, the lack of a categorization system in the trademark context has caused many problems of development and interpretation of the domain name regulation system in recent years.[23] A second important aim of this Article is to identify the limitations of the current domain name system in the political context and to suggest options for future development that would better accommodate the needs of the political process in cyberspace.

Part I deals with situations that may be labeled *political cybersquatting*, where a registrant with no personal connection to a relevant name has registered it in order to sell it for profit to the relevant politician or another person.[24] Part II deals with conduct that may be labeled as *political cyberfraud*, in which an individual or political group registers a relevant domain name to promulgate a misleading message about a politician.[25] This category of conduct may coincide with cybersquatting in some contexts, but the legal issues raised by the two categories of conduct are quite different.[26] Part III deals with the more unusual situation involving competition between trademark holders and politicians with similar names—for example, if Hillary Software, Inc.[27] and Senator Hillary Clinton both wanted the "hillary.com" domain name.[28] Finally, the Article concludes by suggesting options for future developments in political domain name regulation.[29]

---

[21] *See infra* notes 235–236 and accompanying text.

[22] *See infra* notes 351–362 and accompanying text.

[23] *See, e.g.*, Lipton, *supra* note 10, at 1392–38 (discussing examples of utilizing current ill-filling paradigm for certain conduct). *See generally* Jacqueline Lipton, *Commerce Versus Commentary: Gripe Sites, Parody, and the First Amendment in Cyberspace*, 84 WASH. L. REV 1327 (discussing the tension between protecting trademarks and protecting free speech).

[24] *See infra* notes 30–234 and accompanying text.

[25] *See infra* notes 235–362 and accompanying text.

[26] *See infra* notes 235–362 and accompanying text.

[27] Hillary Software, Inc. currently holds the "hillary.com" domain name. *See* Hillary Software, Inc., http://www.hillary.com (last visited Oct. 28, 2007).

[28] *See infra* notes 363–407 and accompanying text.

[29] *See infra* notes 408–424 and accompanying text.

I. Political Cybersquatting

A. *Politicians' Names and the Anticybersquatting Consumer Protection Act*

Political cybersquatting as defined here is the political analog to traditional cybersquatting.[30] It consists of registration and use of a domain name corresponding to a politician's name with the intent to sell the domain name for a profit to the politician or to a third party.[31] Although the conduct is similar—and similarly motivated—in both the trademark and the political contexts, different legal and theoretical issues arise.[32] Traditional cybersquatting occurs when people register often multiple domain names corresponding to registered trademarks with the intent to profit from selling the names to the relevant trademark holders or to a third party.[33] This conduct was originally prohibited under trademark infringement[34] and dilution[35] law. Later, additional regulatory measures were taken to proscribe this conduct.[36] In the United States, the Anticybersquatting Consumer Protection Act

---

[30] *See* Mercer, *supra* note 15, ¶ 4; Dictionary.com, http://dictionary.reference.com/browse/cybersquatting (last visited Oct. 15, 2007) (defining cybersquatting as "the registration of a commercially valuable Internet domain name, as a trademark, with the intention of selling it or profiting from its use"); *see also* 15 U.S.C. § 1129 (2000) (barring cybersquatting relevant to personal names); Nathenson, *supra* note 15, at 925–26 (defining cybersquatting more generally).

[31] *See* Friess, *supra* note 9; Mercer, *supra* note 15, ¶ 4; Nathenson, *supra* note 15, at 925–26.

[32] *See* 15 U.S.C.A. § 1125(d)(1)(A) (West 1998 & Supp. 2007) (regulating bad faith intent to profit from a mark using a domain name); Friess, *supra* note 9 (discussing profit-making intent of political domain name cybersquatters).

[33] *See* Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1319 (9th Cir. 1998) (discussing defendant's domain name registration of over 100 trademarks and his attempt to sell domain names corresponding to marks); Mercer, *supra* note 15, ¶ 4 (defining cybersquatting).

[34] 15 U.S.C. §§ 1114(1)(a), 1125(a)(1) (2000) (prohibiting trademark infringement premised on creation of consumer confusion as to source of relevant goods or services, for registered and common law marks respectively); *see also* Planned Parenthood Fed'n of Am., Inc. v. Bucci, 42 U.S.P.Q.2d (BNA) 1430, 1435–39 (S.D.N.Y. 1997) (using traditional trademark infringement law to prohibit unauthorized bad faith registration and use of a domain name corresponding to the plaintiff's registered trademark).

[35] 15 U.S.C.A. § 1125(c) (prohibiting trademark dilution by blurring, which impairs the distinctiveness of the mark, or tarnishment, which harms the reputation of the mark, regardless of consumer confusion); *see also Panavision*, 141 F.3d at 1324–27 (holding cybersquatter defendant liable for trademark dilution).

[36] Anticybersquatting Consumer Protection Act, Pub. L. No. 106-113, app. I, tit. III, §§ 3001–3010, 113 Stat. 1501A545–A552 (1999) (codified as amended at 16 U.S.C. § 470a (2000); scattered sections of 15 U.S.C.A. (West 1997–98 & Supps. 2007); 28 U.S.C.A. § 1338 (West 2006)).

(the "ACPA") was inserted into the Lanham Act[37] in 1999, to combat this conduct.[38] This legislation prohibits the practice of cybersquatting and sets out a number of "bad faith factors" that courts can use in determining whether particular conduct falls within the notion of a bad faith intent to profit from registration of a relevant domain name.[39]

At roughly the same time, the Internet Corporation for Assigned Names and Numbers (the "ICANN")[40] adopted the Uniform Domain Name Dispute Resolution Policy (the "UDRP")[41] to achieve similar ends. The UDRP has been extremely popular in practice because it is implemented under a private contract between domain name registrants and domain name registrars and hence has a more global reach than domestic legislation.[42] It requires domain name registrants to submit to a mandatory arbitration procedure in the event that someone complains about a bad faith registration or use of a domain name.[43] The arbitrations are fast,[44] inexpensive,[45] and largely online procedures.[46] They can

---

[37] Trademark (Lanham) Act of 1946, 15 U.S.C.A. §§ 1051–1141n (West 1997–1998 & Supps. 2007).

[38] Anticybersquatting Consumer Protection Act, §§ 3001–3010, 113 Stat. at 1501A545–A552.

[39] *Id.*

[40] ICANN is the body that regulates the domain name system. For more information, see Internet Corporation for Assigned Names & Numbers, http://www.icann.org (last visited Oct. 13, 2007).

[41] UDRP, *supra* note 14.

[42] *Id.* ¶ 2 (stating that domain name registrants represent that their registrations "will not infringe upon or otherwise violate the rights of any third party," that a registrant has not "register[ed] the domain name for an unlawful purpose," and "will not knowingly use the domain name in violation of any applicable laws or regulations").

[43] *Id.* ¶ 4(a) (requiring registrants to submit to a mandatory administrative proceeding if a third party complainant asserts to the domain name provider that "(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and (ii) you have no rights or legitimate interests in respect of the domain name; and (iii) your domain name has been registered and is being used in bad faith").

[44] *See* GILSON LALONDE ET AL., *supra* note 18, § 7A.06[3] (discussing potential advantages of the UDRP over the ACPA); InterNIC, FAQs on the Uniform Domain Name Dispute Resolution Policy (UDRP), http://www.internic.net/faqs/udrp.html (last visited Oct. 15, 2007) [hereinafter InterNIC FAQs] (stating a domain name arbitration will generally take less time than judicial proceedings, typically around two months for a decision to be issued).

[45] As of 2002, the range of fees for an arbitration was between $1000 and $2000 for a single arbitrator panel and more for a larger panel. *See* InterNIC FAQs, *supra* note 44.

[46] ICANN, Rules for Uniform Domain Name Dispute Resolution Policy ¶ 3(b), http://www.icann.org/udrp/udrp-rules-24oct99.htm (last visited Oct. 15, 2007) [hereinafter UDRP Rules] (stating complaint should be submitted in hard copy and electronic format); *id.* ¶ 5(b) (requiring response to be submitted in hard copy and electronic format); *id.* ¶ 13

result in transfer of a domain name to a rightful owner if the complainant can establish to the arbitration panel's satisfaction, among other elements, that the registration or use of the domain name was in bad faith and that the registrant had no legitimate purpose for registering the name.[47]

Political cybersquatting, however, is not always covered by these rules, particularly if the politician's name in question is not considered to be trademarked or trademarkable,[48] or if the use of the relevant

---

(prohibiting in-person hearings except in the panel's discretion for an exceptional matter); *id.* ¶ 16(b) (requiring panel decisions to be posted on panel web site).

[47] UDRP, *supra* note 14, ¶ 4(a)(iii), (b), (c) (describing respondent's opportunity to show a legitimate interest to the domain name); *id.* § 4(i) (providing for cancellation or transfer of domain name as remedies available to complainants).

[48] *See id.* ¶ 4(a)(i) (stating that to prevail the domain name must be identical or confusingly similar to a trademark or service mark in which the complainant has rights). A particular politician's name may not be trademarked or trademarkable either at common law or through the federal trademark legislation. *See supra* note 18 (noting that personal names are often not registrable as trademarks and must acquire secondary meaning to be protectable). Nevertheless, personal names may receive some protection as common law marks. *See* Roberts v. Boyd, No. D2000-0210, ¶ 6 (WIPO May 29, 2000), http://www.wipo.int/amc/en/domains/decisions/word/2000/d2000-0210.doc, *reprinted in* WIPO Arbitration & Mediation Ctr., Collection of WIPO Domain Name Panel Decisions 24 (Eun-Joo Min & Mathias Lillengen eds., 2004) (accepting that the movie actress Julia Roberts had common law trademark rights in her personal name for the purposes of a UDRP proceeding). However, this may well be limited mainly to celebrity names that function as trademarks because of their commercial value, as opposed to politicians' names that may well be used more in the political arena than the commercial arena. *See* Friends of Kathleen Kennedy Townsend v. Birt, No. D2002-0451, ¶ 4(b) (WIPO July 31, 2002), http://www.wipo.int/amc/en/domains/decisions/word/2002/d2002-0451.doc (noting prior decision had determined politician Kathleen Kennedy Townsend would not have a common law trademark in her personal name used for political rather than commercial purposes). Additionally, UDRP arbitrators do not regard all famous celebrities as unquestionably holding common law trademark rights in their personal names. *See* Springsteen v. Burgar, No. D2000-1532, ¶ 6 (WIPO Jan. 5, 2001), http://www.wipo.int/amc/en/domains/decisions/word/2000/d2000-1532.doc) (suggesting the singer Bruce Springsteen did not have a common law trademark right in his name for UDRP arbitration purposes, but deciding the matter on other grounds). The tenuous availability of common law trademark rights in celebrities' personal names may be one reason for the growing popularity of the right of publicity tort to protect personal names against unauthorized commercial uses. There is ample scholarship discussing modern applications of the publicity right and critiques of the theories underlying the right. *See generally* Stacey L. Dogan & Mark A. Lemley, *What the Right of Publicity Can Learn from Trademark Law*, 58 Stan. L. Rev. 1161 (2006) (discussing modern expansion of the right of publicity and the various theories underlying the right); Sarah M. Konsky, *Publicity Dilution: A Proposal for Protecting Publicity Rights*, 21 Santa Clara Computer & High Tech. L.J. 347 (2005) (proposing right of publicity dilution to replace currently broad right of publicity); Mark P. McKenna, *The Right of Publicity and Autonomous Self-Definition*, 67 U. Pitt. L. Rev. 225 (2005) (criticizing current justifications of the right of publicity and proposing a right of autonomous self-definition).

name is not of a trademark-infringing kind.[49] That political cybersquatting will not be covered if the name is not trademarked or trademarkable will certainly be true of traditional trademark infringement[50] and dilution actions,[51] and also of general trademark-based anticybersquatting actions under the ACPA.[52] Although some additional anticybersquatting laws do deal specifically with the protection of individuals' names against bad faith cybersquatting even in the absence of a trademark interest in the name,[53] they may be limited in application. The obvious example of an anticybersquatting law that protects nontrademarked personal names against cybersquatting is 15 U.S.C. § 1129, introduced in 1999, as part of the ACPA.[54] It provides:

> Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.[55]

---

[49] *See* Trademark (Lanham) Act of 1946, 15 U.S.C. §§ 1114(1), 1125(a)(1) (2000) (prohibiting trademark infringement premised on creation of consumer confusion as to source of relevant goods or services for registered and common law marks respectively). Therefore, the use may not be a trademark-infringing kind if it does not implicate confusion as to source of goods or services. *See id.* Even an unregistered mark or common law mark will only receive protection to the extent that it functions as a mark and is capable of distinguishing the source of goods or services to which the mark is attached. *Id.* § 1125(a)(1) (protecting common law marks against false and misleading use "in connection with the sale of goods or services"); *see also* GILSON LALONDE ET AL., *supra* note 18, § 2.01 (discussing marks' ability to distinguish source as crucial to protectibility).

[50] *See* 15 U.S.C. §§ 1114(1), 1125(a)(1).

[51] *See* 15 U.S.C.A. § 1125(c) (West 1998 & Supp. 2007) (prohibiting dilution through blurring, defined as harming the ability of a mark to distinguish its source, or tarnishment, defined as harming the mark's reputation).

[52] *See id.* § 1125(d) (prohibiting cybersquatting based on registration of a domain name similar to a trademark).

[53] *See id.* § 1129 (protecting against cybersquatting personal names not limited to trademark, or trademarkable, interests).

[54] Anticybersquatting Consumer Protection Act, Pub. L. No. 106-113, app. I, tit. III, §§ 3001–3010, 113 Stat. 1501A545–A552 (1999) (codified as amended at 16 U.S.C. § 470a (2000); scattered sections of 15 U.S.C.A. (West 1997–98 & Supps. 2007); 28 U.S.C.A. § 1338 (West 2006)). Section 1129 is to be distinguished from 15 U.S.C.A. § 1125(d), a subsection also added by the ACPA but which is restricted to prohibitions on bad faith cybersquatting where the cybersquatter has registered a domain name that is similar to a trademark, as opposed to a personal name as in § 1129. *See* 15 U.S.C.A. § 1125(d); 15 U.S.C. § 1129.

[55] 15 U.S.C. § 1129(1)(A). This provision is in some ways broader than the general trademark protections for personal names under the Lanham Act. Although personal names

This provision will cover some, but not all political cybersquatting. If the ACPA had been applied to the "kerryedwards.com" scenario,[56] for example, the candidates could have argued that the "kerryedwards.com" name violated the statute because it was substantially similar to that of another living person and that the defendant intended to profit from selling the domain name.[57] But it might technically have been possible for the registrant, Mr. Kerry Edwards, to mount several defenses to an ACPA challenge.[58] He might have argued that the domain name in question did not actually correspond to the name of another living person because "Kerry Edwards" was not the name of either Senator Kerry or Senator Edwards, but rather an amalgam of both of their names.[59] He might also have argued that, even if the name in question did consist of the name of another living person, it also consisted of his own personal name—Kerry Edwards—and that his own right to a domain name corresponding to his personal name must be protected equally by § 1129.[60]

With respect to the first argument—that the name "kerryedwards.com" does not correspond to the name of an actual living person—Mr. Kerry Edwards's defense against the ACPA could fail on the ground that § 1129 also protects complainants against bad faith registrations of domain names that are "substantially and confusingly similar" to their own personal names.[61] Arguably, the amalgam of the names Kerry and Edwards in "kerryedwards.com" in the lead-up to a presidential election where Senators Kerry and Edwards's names are those on the presidential ticket would be considered a registration of a name "substantially and confusingly similar" to the senators' respec-

---

are trademarkable with the consent of the relevant person, they have to serve as trademarks—as source identifiers of goods or services—in order to retain their trademark status and registration. *See* 15 U.S.C. § 1052(c) (2000). On the other hand, 15 U.S.C. § 1129(1)(A) does not require a "trademark use" of a personal name in order for it to be protected against someone who registers a corresponding domain name with a financial profit motive. *Id.* § 1129(1)(A). It may be that this difference can be explained by the idea that a sale of a domain name for profit is akin to sale of a good or service bearing the relevant personal name as a trademark.

[56] *See* Posting of Betrand Pecquerie to The Editors Weblog, *Kerry Edwards Is Real and Sells Kerryedwards.com*, http://wef.blogs.com/editors/2004/07/index.html (July 19, 2004 23:27 EST) (quoting Frank Barnako, *KerryEdwards.com Is Fielding Bids*, MARKETWATCH, July 19, 2004, http://www.marketwatch.com/news/story/kerryedwardscom-goes-auction-block/story.aspx?guid=%7B42DE0C46%2D47C3%2D4AF3%2DB9EA%2D0B9E448CDAB1%7).

[57] *See* 15 U.S.C. § 1129.

[58] *See id.*

[59] *See id.*

[60] *See id.*

[61] *See id.* § 1129(1)(A).

tive personal names.[62] The second potential defense—that § 1129 protects Mr. Kerry Edwards's right to a domain with his own personal name—may be more likely to succeed.[63] Nevertheless, a court taking at least an economic analysis of the situation may well find that the use of the name for a presidential campaign would be less socially and economically wasteful than the use of a name by a person with a corresponding personal name who is simply trying to make a profit from selling that name.[64]

There were two unusual factors about the "kerryedwards.com" situation that may well not be repeated in many future cases. For one thing, Mr. Kerry Edwards happened fortuitously to have registered the domain name several years before the presidential campaign featuring Senators Kerry and Edwards was launched.[65] Thus, in this particular case, had the senators brought an action against Mr. Kerry Edwards, they may well have failed on the basis that he had not *registered*—as opposed to having used—the domain name with the intent to profit from its sale, as required by § 1129.[66] The other factor, which is of course related to this first factor, is that Mr. Kerry Edwards happened to have a personal name that corresponded to the two names on the presidential ticket.[67] This is unlikely to happen in many future cases. It is possible, however, that a private individual might have a personal name corresponding to an individual politician's name in a future campaign, and this could raise many of the difficulties that might have arisen had "kerryedwards.com" been litigated in the lead-up to the 2004 presidential election. How many John McCains are out there, for example, or Joe Bidens, or Chris Dodds? In this respect, politicians with unusual personal names may have big advantages over those with more common names—make way for Arnold Schwarzenegger and Rudy Giuliani,

---

[62] *See* 15 U.S.C. § 1129(1)(A).

[63] *See id.*

[64] *See id.*

[65] *See* Pecquerie, *supra* note 56.

[66] *See* 15 U.S.C. § 1129(1)(A) ("Any person who *registers a domain* name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, *with the specific intent to profit* from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.") (emphasis added); Pecquerie, *supra* note 56. Section 1125(d) would not have applied here because the "Kerry Edwards" name was not trademarked, nor was it likely trademarkable in the electoral context. *See* 15 U.S.C. § 1052(c) (2000); 15 U.S.C.A. § 1125(d) (West 1998 & Supp. 2007). Generally, personal names are not registrable as trademarks. 15 U.S.C. § 1052(c); *see also* GILSON LALONDE ET AL., *supra* note 18, § 2.03[4][d] (discussing requirement of secondary meaning for personal name protection).

[67] Barnako, *supra* note 56.

not to mention Barack Obama.[68] It obviously does not make sense that unusual political names should fortuitously receive more protection than more common names in the domain space.

Other than the relatively unusual situation where a private individual's name corresponds to a relevant domain name, there are a few other practical problems with the ACPA provisions protecting personal names from bad faith registrations.[69] One problem is that the ACPA does not have a global reach, although a federal statute at least is better in terms of legal harmonization than a pastiche of often-piecemeal state laws.[70] Another potential problem with § 1129 is an arguable general lack of familiarity with its provisions, partly perhaps because they have been overshadowed by the UDRP, which covers much of the same ground as the ACPA in a quick, inexpensive, efficient, and, of course, global manner.[71] Since the introduction of both the ACPA and the UDRP in 1999, many more complaints have been brought under the UDRP than the ACPA, even with respect to names of private individuals.[72] This is not surprising, but, as recent UDRP

---

[68] Although, illustrating the international reach of this issue, obama.com, for example, appears to be registered to an Obama Satoru of Japan. *See* Whois.net, WHOIS Information for Obama.com, http://whois.net/whois_new.cgi?d=obama&tld=com (last visited Oct. 12, 2007).

[69] 15 U.S.C. § 1129.

[70] *See id.*; CAL. BUS. & PROF. CODE § 17525(a) (West 1997 & Supp. 2007); CAL. ELEC. CODE §§ 18320–18383 (West 2003 & Supp. 2007).

[71] *See supra* notes 40–47 and accompanying text.

[72] *See e.g.*, Clinton v. Dinoia a/k/a SZK.com, No. FA0502000414641 (NAF Mar. 18, 2005), http://www.arb-forum.com/domains/decisions/414641.htm (involving the domain name "hillaryclinton.com"); Townsend v. Birt, No. D2002-0030, ¶ 6 (WIPO Apr. 11, 2002) (failing to protect politician Kathleen Kennedy Townsend's name under the UDRP); *Springsteen*, No. D2000-1532, ¶ 6 (finding brucespringsteen.com should not be transferred from the Bruce Springsteen Club to the musician Bruce Springsteen because none of the required elements in UDRP ¶ 4(b) were satisfied); Ciccone v. Parisi, No. D2000-0847, ¶ 7 (WIPO Oct. 12, 2000), http://www.wipo.int/amc/en/domains/decisions/word/2000/d2000-0847.doc, *reprinted in* WIPO ARBITRATION & MEDIATION CTR., *supra* note 48, at 74 (transferring domain name madonna.com to singer Madonna based on her rights in the registered trademark); Helen Folsade Adu, known as Sade v. Quantum Computer Servs. Inc., No. D2000-0794, ¶ 6 (WIPO Sep. 26, 2000), http://www.wipo.int/amc/en/domains/decisions/word/2000/d2000-0794.doc (finding trademark interest in performing artist Sade's stage name); Rita Rudner v. Internetco Corp., No. D2000-0581, ¶ 5 (WIPO Aug. 3, 2000), http://www.wipo.int/amc/en/domains/decisions/word/2000/d2000-0581.doc (concluding Rita Rudner had a common law trademark interest in her personal name); *Roberts*, No. D2000-0210, ¶¶ 6, 7 (concluding Julia Roberts had a common law trademark in her name and transferring "juliraroberts.com" to her). On the other hand, few reported cases have emerged from § 1129. *See* 15 U.S.C.A. § 1129 annots. (citing only Hammer v. Amazon.com, 392 F. Supp. 2d 423 (E.D.N.Y. 2005) and Schmidheiny v. Weber, 285 F. Supp. 2d 613 (E.D. Pa. 2003)). A comparison of the UDRP disputes suggests that it is far from clear that UDRP arbitrators at least will always find the existence of a trademark corresponding

arbitrations have shown, the UDRP is not as easily geared as § 1129 to combat cybersquatting involving *any* personal names, let alone political personal names.[73]

B. *Politicians' Names and the Uniform Domain Name Dispute Resolution Policy*

The UDRP contains certain procedural advantages for a complainant concerned with an act of bad faith cybersquatting.[74] Its main limitation in the context of political cybersquatting is that it does not specifically protect personal names against bad faith registrations and uses.[75] This does not mean that no private individuals have attempted to utilize the UDRP to protect their interests in relevant domain names. In fact, some celebrities have been quite successful in this context.[76] Even some politicians have succeeded here.[77] The problem has been that, in the absence of specific protection for personal names under the UDRP, complainants must successfully assert a trademark interest in their personal names.[78] This can sometimes be done quite easily: for example, some celebrities do hold registered trademarks in their names if they use them as commercial trademarks.[79] In other cases, UDRP arbitrators

---

to a famous personal name, as in *Springsteen v. Burgar*. *See* No. D2000-1532, ¶ 6 (suggesting it was not clear that the UDRP was meant to protect a proper name like Bruce Springsteen's but assuming the name was protectible for subsequent discussion).

[73] *See* UDRP, *supra* note 14, ¶ 4(a)–(b); *see also Townsend*, No. D2002-0030, ¶ 6 (failing to protect politician Kathleen Kennedy Townsend's name under the UDRP); *Springsteen*, No. D2000-1532, ¶ 6.

[74] *See* GILSON LALONDE ET AL., *supra* note 18, § 7A.06[3]; InterNIC FAQs, *supra* note 44; *supra* notes 44–47 and accompanying text.

[75] *See* UDRP, *supra* note 14, ¶ 4(a)(i).

[76] *E.g.*, *Ciccone*, No. D2000-0847, ¶¶ 4, 7; *Roberts*, No. D2000-0210, ¶¶ 6–7.

[77] *Clinton*, No. FA0502000414641 (involving the domain name "hillaryclinton.com").

[78] UDRP, *supra* note 14, ¶ 4(a)(i) (stating complainant must establish trademark interests corresponding to relevant domain name as one of the bases for her complaint). This was certainly played out in domain name disputes corresponding to the personal names of Julia Roberts, Madonna, and Hillary Clinton, where UDRP arbitrators established that all of these people had trademark interests in their personal names to support their UDRP complaints. *See Clinton*, No. FA0502000414641; *Ciccone*, No. D2000-0847, ¶¶ 4, 7; *Roberts*, No. D2000-0210, ¶ 6.

[79] For example, the singer Madonna has registered Madonna as a trademark. *Ciccone*, No. D2000-0847, ¶ 4 ("Complainant is the well-known entertainer Madonna. She is the owner of U.S. Trademark Registrations for the mark MADONNA for entertainment services and related goods (Reg. No. 1,473,554 and 1,463,601). She has used her name and mark MADONNA professionally for entertainment services since 1979.").

have been prepared to accept common law trademark rights in a famous celebrity's[80] or politician's name.[81]

Even in the case of celebrities' or politicians' famous personal names, however, UDRP arbitrators do not always find a trademark interest on the part of the complainant.[82] When Bruce Springsteen and his management initiated a UDRP arbitration for transfer of the "springsteen.com" name from a registrant utilizing it to link to his own celebrities website, the majority arbitration panelists were not convinced that a celebrity, even one as popular as Springsteen, necessarily had a common law trademark right in his personal name.[83] Similarly, in the political context, Kathleen Kennedy Townsend failed to convince UDRP arbitrators that she had a trademark interest in her personal name in the context of a gubernatorial election in Maryland in which she was a candidate.[84] Interestingly, the panel suggested that supporters of Townsend may have been able to assert a trademark interest in her name,[85] and that Townsend herself may have successfully brought an action under § 1129 which would not have required her to establish even a

---

[80] *See Roberts*, No. D2000-0210, ¶ 6 ("Having decided that Complainant has common law trademark rights in her name, the next consideration was whether the domain name <juliaroberts.com> was identical to or confusingly similar with Complainant's name.").

[81] *E.g.*, *Clinton*, No. FA0502000414641 ("The Panel finds that Complainant's uncontested allegations establish common law rights in the HILLARY CLINTON mark sufficient to grant standing under the UDRP. Complainant alleges that the HILLARY CLINTON mark has become distinctive through Complainant's use and exposure of the mark in the marketplace and through use of the mark in connection with Complainant's political activities, including a successful Senate campaign.").

[82] *Springsteen*, No. D2000-1532, ¶ 6.

[83] *Id.* ¶¶ 1–5, 6 (noting that "[i]t is common ground that there is no registered trade mark in the name 'Bruce Springsteen'" and the name would be impossible to register in most jurisdictions, and requiring Mr. Springsteen to rely on common law rights to satisfy the elements in the UDRP's three part test). The panel majority emphasized that there was no evidence that the name "Bruce Springsteen" had acquired secondary meaning, "in other words a recognition that the name should be associated with activities beyond the primary activities of Mr. Springsteen as a composer, performer, and recorder of popular music." *Id.* Thus the panel found it "by no means clear" that the UDRP was intended to protect such names. *Id.*

[84] *Townsend*, No. D2002-0030, ¶ 6 (involving Kathleen Kennedy Townsend's name and finding "that the protection of an individual politician's name, no matter how famous, is outside the scope of the Policy since it is not connected with commercial exploitation as set out in the Second WIPO Report").

[85] *Id.* ("Here, the claim for the domain names is brought by the individual politician, and not by the political action committee actively engaged in the raising of funds and promotion of Complainant's possible campaign. Had the claim been brought in the name of the Friends of Kathleen Kennedy Townsend, the result might well have been different. But it was not.").

common law mark in her personal name.[86] From these examples, it seems that politicians' names used in the context of political campaigns may not merit any form of trademark protection,[87] and that even some nonpolitical celebrity names may not merit even common law protection as trademarks.[88]

It has been suggested that the UDRP be revised to incorporate provisions protecting personal names from bad faith registration and use.[89] To date, however, no revisions have been made, and the World Intellectual Property Organization (the "WIPO") has suggested further inquiry into the need for such revisions.[90] One should bear in mind that the UDRP is a global arbitration process.[91] The protection of personal names on a global scale may well raise a number of greater difficulties than adopting such provisions at the domestic level,[92] such as in § 1129.[93] On the global scale, there are more names and presumably more people, even potentially famous people, with the same or similar names.[94] Additionally, different legal systems may well take differing attitudes to the protection of personal names in the domain space, whether they be politicians', celebrities', or private individuals' names.

---

[86] *Id.* ("This does not mean that Complainant is without remedy. The ACPA contains express provisions protecting the rights in personal names."). It is not clear from the record why Townsend did not pursue a § 1129 action.

[87] This may make sense if we assume that the purpose of most trademark law and trademark-related actions is to prevent consumer confusion with respect to the source of goods or services.

[88] *See Springsteen*, No. D2000-1532, ¶ 6.

[89] WORLD INTELLECTUAL PROP. ORG., SECOND WIPO INTERNET DOMAIN NAME PROCESS: THE RECOGNITION OF RIGHTS AND THE USE OF NAMES IN THE INTERNET DOMAIN NAME SYSTEM, Sept 3, 2001, ¶¶ 189–204, http://www.wipo.int/amc/en/processes/process2/report/html/report.html#5, [hereinafter WIPO SECOND DOMAIN PROCESS].

[90] *Id.* ¶¶ 202–203 ("It is recommended that no modification be made to the UDRP to accommodate broader protection for personal names than that which currently exists in the UDRP. . . . In making this recommendation, we are conscious of the strength of feeling that the unauthorized, bad faith registration and use of personal names as domain names engenders. We believe, however, that the most appropriate way in which the strength of this feeling should be expressed is through the development of international norms that can provide clear guidance on the intentions and will of the international community.").

[91] *See id.* ¶¶ 199–204.

[92] *See id.*

[93] *See* 15 U.S.C. § 1129 (2000).

[94] For example, obama.com is owned by a Satoru Obama of Japan. *See* Whois.net, *supra* note 68.

C. *Application of Cyberfraud Legislation to Political Cybersquatting*

There are some other possible legal avenues for political actors concerned about political cybersquatting. California's Political Cyberfraud Abatement Act (the "PCAA"), for example, prohibits engaging in acts of "political cyberfraud" that include conduct concerning a political website:

> that is committed with the intent to deny a person access to a political Web site, deny a person the opportunity to register a domain name for a political Web site, or cause a person reasonably to believe that a political Web site has been posted by a person other than the person who posted the Web site . . . .[95]

Some aspects of this provision may cover political cybersquatting, even though it is notionally directed at conduct described as *cyberfraud*.[96] It should be noted that as written, the terms of this statute apply only to websites that urge or appear to urge the support or opposition of ballot measures.[97]

The third statutory category of cyberfraud—causing a person reasonably to believe that a political website has been posted by a person other than the person who posted the website—likely does not cover political cybersquatting as defined in this Article.[98] This is because the point of cybersquatting is to sell the domain name for a profit rather than to make misleading use of the site.[99] It is, of course, possible that a domain name registrant could use a domain name for both purposes—that is, disseminating misleading information about a campaign and at the same time trying to sell the domain name. But the "misleading information" component of such conduct is categorized throughout this Article as *political cyberfraud* rather than *political cybersquatting* because there is a need to separate and categorize different types of conduct relating to political domain names in order to provide appropriately tailored legal solutions for relevant conduct.

The first two prohibitions in the California PCAA, however, could potentially cover some political cybersquatting.[100] Registering a political domain name with the intention of selling it for profit could potentially amount to conduct intended to deny a person access to a political web-

---

[95] CAL. ELEC. CODE § 18320(b), (c)(1) (West 2003 & Supp. 2007).

[96] *See id.* § 18320(c)(1)(A) (defining and prohibiting political cyberfraud).

[97] *See id.* § 18320(c)(3).

[98] *See id.* § 18320(c)(1).

[99] *See id.*

[100] *See* CAL. ELEC. CODE § 18320 (c)(1).

site or to deny a person the opportunity to register a domain name for a political website.[101] The PCAA further illustrates that the political cyberfraud activities it covers include, but are not limited to, the following examples:

> (A) Intentionally diverting or redirecting access to a political Web site to another person's Web site by the use of a similar domain name . . . .[102]
> (C) Registering a domain name that is similar to another domain name for a political Web site.[103]
> (D) Intentionally preventing the use of a domain name for a political Web site by registering and holding the domain name or by reselling it to another with the intent of preventing its use, or both.[104]

These are all examples of conduct that could deny a political actor access to a relevant domain name.[105] Nevertheless, conduct that could deny access to a website and that fits these prohibitions may not technically amount to political cybersquatting as defined here.[106] In situations where the political actor in question has not yet registered a relevant domain name, it would be difficult to argue that access was being "diverted" or "redirected" from that person's website to another website.[107] If the campaign never had a website to begin with, this provision may have no application.[108] Nevertheless, it may well apply to a situation where a political actor does have a website but has not registered all possible permutations of the relevant domain name.[109]

For example, Senator Barack Obama has registered "barackobama.com," but at the time of writing does not appear to have registered "barack.com" or "obama.com" himself.[110] If someone else were to register either of these names, Senator Obama could complain under a statute similar to the PCAA on the basis that the name diverts

---

[101] *See id.*
[102] *Id.* § 18320(c)(1)(A).
[103] *Id.* § 18320(c)(1)(C).
[104] *Id.* § 18320(c)(1)(D).
[105] *See id.* § 18320(c)(1), (3).
[106] *See* CAL. ELEC. CODE § 18320(c)(1)(A).
[107] *See id.*
[108] *See id.*
[109] *See id.*
[110] *See* Register.com, Whois Domain Name Lookup for www.barack.com, http://www.register.com/whois_info.rcmx?requestType=validate_challenge (last visited Oct. 13, 2007) (stating barack.com is registered to a Doron Barack in Israel); Whois.net, *supra* note 68 (stating that obama.com is registered to an individual by the name of Obama in Japan).

web users from his own website. Presumably, he would have to prove actual diversion rather than, for example, a likelihood of diversion.[111] It is not clear what proof would be necessary in this context. Could he simply prove that consumers were initially confused by typing the wrong domain name into their web browser and ending up at the wrong website, even if they were not thereafter prevented from finding his site through use of their browsers or search engines?[112]

Similar comments may be made about subsection (C). A statutory provision that covers all politicians and prohibits "[r]egistering a domain name that is similar to another domain name for a political website" still may not include situations where the politician in question has not yet registered a domain name corresponding to her personal name.[113] But where the politician in question already does have a web presence, this type of provision may be more useful than a prohibition on redirecting or diverting as in subsection (A). This is because it requires only registration of a name that is similar to an existing political domain name, not proof of intent to divert or redirect access to the site, which is likely a more difficult task.

Subsection (D) looks to be directed much more at the kind of conduct described in this Article as "political cybersquatting" than the other provisions.[114] It prohibits "intentionally preventing the use of a domain name for a political website by registering and holding the domain name or by reselling it to another with the intent of preventing

---

[111] *Cf.* 15 U.S.C. § 1125(a) (2000) (prohibiting trademark infringement that causes a likelihood of confusion).

[112] This would be similar to the "initial interest confusion" doctrine that has arisen in the commercial trademark context, with a domain name registrant effectively confusing a "search engine" rather than an Internet user as to the relationship between a domain name and a trademark. *See* Brookfield Commc'ns, Inc. v. West Coast Entm't Corp., 174 F.3d 1036, 1062–64 (9th Cir. 1999) (considering initial interest confusion when search engines divert to competitors' domain names due to use of the trademark in metatags); *cf. Panavision*, 141 F.3d at 1327 (holding that although consumers would not actually have been confused as to source by defendant's website, they may be discouraged from finding the plaintiff's actual web presence, resulting in dilution). Even though Internet users would not necessarily be confused once they arrived at the site they were not actually searching for, courts have been prepared to find the "consumer confusion" requirement of trademark infringement law made out on the basis of the notion of "initial interest confusion." *See Brookfield*, 174 F.3d at 1062–64; *see also* Eric Goldman, *Deregulating Relevancy in Internet Trademark Law*, 54 EMORY L.J. 507, 559 (2005) ("[Initial interest confusion] lacks a rigorous definition, a clear policy justification, and a uniform standard for analyzing claims. With its doctrinal flexibility, [it] has become the tool of choice for plaintiffs to shut down junior users who have not actually engaged in misappropriative uses.").

[113] *See* CAL. ELEC. CODE § 18320(c)(1)(C) (West 2003 & Supp. 2007).

[114] *See id.* § 18320(c)(1)(D).

its use, or both."[115] This does not appear to require the prospective political speaker to have already registered any domain name for the statute to apply.[116] It would potentially cover a situation where a political speaker was prevented from registering a name she wanted as a domain name by a registrant who either holds on to the name and does not resell it, or by a registrant who sells the name with the intent to prevent its use by the speaker.[117]

The drafting of this provision, however, may still be somewhat problematic in the situations described here as political cyber-squatting. The provision does not cover situations where the registrant of the domain name is prepared to sell the domain name for a profit. It only appears to cover situations where the registrant is attempting to prevent the name from actually being used. Thus, it could cover the situation where the registrant of "barack.com" either wasted an important political resource by simply holding it and not using it, or where the registrant attempted to sell it to someone else who might prevent Senator Obama from using it. But the prohibition does not seem to contemplate the type of conduct where the registrant specifically attempts to sell the name for actual use, such as to sell "barack.com" to Senator Obama for a profit.[118]

There are also jurisdictional problems with the application of the PCAA, as there would be with any potential analogous state statute. Currently, California is the only state with such legislation.[119] It is not clear whether this legislation would apply in situations where neither the political actor nor the domain name registrant is located in California.[120] It is possible that the ability of web users to access the website in California would be a sufficient connection with California for the PCAA to apply.[121] Additionally, it is possible that registering the

---

[115] *See id.*

[116] *See id.*

[117] *See id.* § 18320(a)(1), (c).

[118] Thus as written it would probably not cover the individuals who rent out recurring ballot measure websites to various interested parties. *See* Friess, *supra* note 9.

[119] *See* Pereira, *supra* note 12, at 406 (noting that until the PCAA and sections 17525–17526 of the Business and Professions Code, no law addressed political websites).

[120] The PCAA notes that jurisdiction should be exercised consistent with the jurisdictional provision in the California Code of Civil Procedure, which in turn is coextensive with the constitutions of the United States and California. *See* CAL. CIV. PROC. CODE § 410.10 (West 2004); CAL. ELEC. CODE § 18323.

[121] Nevertheless, case law also suggests that the mere ability to access a website within a jurisdiction, without more, is an insufficient basis at least for the assertion of personal jurisdiction against an out-of-state defendant website operator. *See, e.g.*, Bensusan Restaurant Corp. v. King, 937 F. Supp. 295, 299 (S.D.N.Y. 1996) (holding defendants who operated a

domain name in California would be sufficient grounds to apply California law.[122] If this were the case, however, clever domain name cybersquatters would simply select a domain name registrar not situated in California.[123]

Maybe if political cybersquatting is regarded as a sufficiently important activity for regulation at the federal or global level, certain ideas could be taken from the California legislation and incorporated into either a federal statute or global treaty. Alternately, at the global level, some of these ideas could be incorporated into a dispute resolution procedure such as the UDRP.[124] Domain name registrants could contractually agree with registrars that they would submit to an arbitration procedure not unlike the UDRP if a politician, or perhaps political party,[125] later complained about registration of the relevant name, particularly in the context of an election. New bad faith factors could be incorporated in such a revised dispute resolution procedure. These factors could be borrowed to some extent from the PCAA and could be further expanded to cover situations where a politician has not yet registered any domain names.[126] They should also cover situations where the registrant attempts to sell the domain name to the politician or a third party. This approach may be quicker, cheaper, and more efficient than federal legislation or an international treaty, particularly a treaty requiring implementing legislation.

---

jazz club in Missouri could not be subject to personal jurisdiction in New York, where the only conduct connected with the forum was advertising their Missouri club on a website that was accessible in New York City, but that was not specifically directed to New York City residents), *aff'd* 126 F.3d 25 (2d Cir. 1997).

[122] The ACPA, for example, is a domain name law that includes in rem jurisdiction provisions in the case of domain names registered in a particular jurisdiction where the plaintiff is not otherwise able effectively to assert personal jurisdiction over the defendant domain name registrant. 15 U.S.C.A. § 1125(d)(2)(A) (West 1998 & Supp. 2007).

[123] For example, a list of ICANN-accredited domain name registrars from all over the world is available at http://www.icann.org/registrars/accredited-list.html (last visited Oct. 14, 2007).

[124] *See generally* UDRP, *supra* note 14.

[125] Political parties may, in fact, be in a better position than politicians under the UDRP as currently drafted. *See Townsend*, No. D2002-0030, ¶ 6 ("Here, the claim for the domain names is brought by the individual politician, and not by the political action committee actively engaged in the raising of funds and promotion of Complainant's possible campaign. Had the claim been brought in the name of the Friends of Kathleen Kennedy Townsend, the result might well have been different. But it was not."). *But see Friends of Kathleen Kennedy Townsend*, No. D2002-0451, ¶ 5 (denying standing to Townsend's committee and suggesting there was no trademark use).

[126] *See* CAL. ELEC. CODE § 18320(c)(1) (West 2003 & Supp. 2007).

D. *Political Cybersquatting, Defamation Law, and the Right of Publicity*

Another group of laws that may apply to political cybersquatting conduct, albeit somewhat indirectly, are various tort laws that protect individual reputations from harmful conduct.[127] These include defamation law, the right of publicity,[128] and some *sui generis* state legislation such as the California Business and Professions Code sections 17525 and 17526.[129]

1. Defamation

The most obvious tort that deals with a person's reputation is defamation.[130] Defamation generally refers to false statements that damage an individual's reputation.[131] Although defamation may be relevant to variations of the conduct described in this Article as *political cyberfraud*, it likely has little to no application to political *cybersquatting*. This is because cybersquatting does not deal with any statements that might damage an individual politician's reputation.[132] Rather, cybersquatting removes from the politician's ready accessibility a domain name that the politician might need to make statements in support of his campaign. Thus, although defamation may be somewhat relevant to political cyberfraud, it need not be discussed further with respect to political cybersquatting.

2. The Right of Publicity

The state right of publicity, on the other hand, could apply to political cybersquatting.[133] The right of publicity has been described as "the right of an individual to control the commercial use of his or her

---

[127] *See infra* notes 133–176 and accompanying text.

[128] Michael Madow, *Personality as Property: The Uneasy Case for Publicity Rights*, *in* 3 INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE 345, 345–51 (Peter Yu ed., 2007) (explaining that the right to publicity "gives a celebrity a legal entitlement to the commercial value of her identity, and thereby enables her to determine the extent, manner, and timing of its commercial exploitation").

[129] *See* CAL. BUS. & PROF. CODE § 17525(a) (West 1997 & Supp. 2007); *infra* notes 177–200 and accompanying text.

[130] *See* Janet L. Silverberg, *Commercial Defamation and Trade Libel*, *in* 1 BUSINESS TORTS ¶ 6.01 (Joseph D. Zamore ed., 2007).

[131] *Id.*

[132] *See* 15 U.S.C.A. § 1125(d)(1) (West 1998 & Supp. 2007); *see also* Dictionary.com, http://dictionary.reference.com/browse/cybersquatting (defining cybersquatting as "the registration of a commercially valuable Internet domain name, as a trademark, with the intention of selling it or profiting from its use") (last visited Oct. 12, 2007).

[133] *See* Madow, *supra* note 128.

name, likeness, signature, or other personal characteristics."[134] Some have likened it to a trademark-like right in a famous person's attributes in the sense that it protects the goodwill inherent in that person's commercial persona.[135] The right of publicity operates much like a trademark in the sense that it "reserves to an individual celebrity the exclusive right to the commercial exploitation of his or her name, likeness, signature, or product endorsement."[136]

To determine whether the right of publicity might have any application in the political cybersquatting context, two fundamental questions must be answered. The first is whether the registration of a domain name corresponding to a politician's name for the purposes of commercial profit amounts to a "commercial exploitation"[137] of the politician's name in the manner contemplated by the law. The second is whether the right of publicity in the context of purely political campaigns, as distinct from other more commercial activities, protects politicians. No state or federal court or legislature in the United States has definitively answered either question. Additionally, this approach is limited because the right of publicity is not accepted in all American states,[138] let alone globally.

It is not clear whether the commercial sale or attempted sale of a domain name that corresponds to a politician's name is the kind of conduct generally contemplated within the right of publicity. Usually, the actions brought under this tort are concerned with the sale of specific items—photographs, tee-shirts, magazines, toys, etc.—that contain,

---

[134] GILSON LALONDE ET AL., *supra* note 18, § 2.16[1].

[135] *Id.* ("The right of publicity is analogous to the right in a trademark. Both are exclusionary in nature, giving rise to injunctive relief and possible damages when they are violated, and both depend for their value to a great degree on public recognition, perception, and association. The goodwill which a trademark symbolizes is a first cousin to the goodwill, or reputation and fame, of the celebrity. These establish the commercial value of the right to be protected, a value which in either case can be enormous. They significantly enhance the sales potential of the trademarked or celebrity-endorsed products with which they are associated, and can create a formidable competitive advantage.").

[136] *Id.* § 2.16[1][b].

[137] *Id.*

[138] *Id.* § 2.16[1] ("The publicity right is still developing and the courts are far from unanimous in defining its scope. Precedent (or the lack of it) in the selected forum may thus dictate reliance on trademark rights and unfair competition claims to the exclusion of, or in addition to, the publicity right. In either case the celebrity may rely on his or her federal registration, Section 43(a), common law unfair competition, and the same assortment of state statutes that are available in infringement actions involving other types of marks.").

or are based on, an unauthorized likeness of a famous celebrity.[139] On the one hand, the sale of a domain name that corresponds to a famous celebrity's name may well be likened to the sale of a product that contains or constitutes the name or likeness of the person in question. On the other hand, could the sale of an unauthorized photograph, teeshirt, or coffee mug bearing the name or likeness of, say, Britney Spears, really be likened to the sale of a blank web page with the domain name "britney.com," or even "britneyspears.com"? In the case of the physical goods, it would seem more plausible that consumers would be confused as to whether the pop singer had authorized the product line than in the case of a blank webpage utilizing a domain name that corresponds to her name.

Whether or not physical goods are likely to create more confusion, there is still an open question as to whether the right of publicity protects politicians as opposed to celebrities whose notoriety is based on commercial, rather than political, aspects of their persona.[140] This question was recently cast into the limelight in a lawsuit filed by Arnold Schwarzenegger, the governor of California, against a manufacturer of bobblehead dolls bearing his name and likeness.[141] Although

---

[139] *See, e.g.*, Hoffman v. Capital Cities/ABC Inc., 255 F.3d 1180, 1183–89 (9th Cir. 2001) (analyzing use of digitally manipulated image of Dustin Hoffman in magazine under the right of publicity but concluding it was protected by the First Amendment); Allen v. Men's World Outlet Inc., 679 F. Supp. 360, 367–70 (S.D.N.Y. 1988) (holding use of Woody Allen look alike for clothing store advertisements created a likelihood of confusion as a matter of law); Winterland Concessions Co. v. Creative Screen Design Ltd., 210 U.S.P.Q. 6, 8–9 (N.D. Ill. 1980) (issuing injunction against defendant's production of unauthorized teeshirts featuring the names of entertainers' assignee). In this context, celebrity names will often attain a common law trademark status as well. GILSON LALONDE ET AL., *supra* note 18, § 2.16[1] ("[A] celebrity's name or likeness may *itself* be a trademark, if it is used by the celebrity to identify the source of products or services and to distinguish them from those of others. GLORIA VANDERBILT jeans, JIMMY DEAN sausage, REGGIE candy bars, are but a few examples of celebrity-trademarked products. If the celebrity uses the name or likeness in this way, he or she can ordinarily obtain federal registration, so that the name or likeness will enjoy the registration benefits provided by the [Lanham] Act.").

[140] *See, e.g.*, Martin Luther King, Jr., Ctr. for Soc. Change, Inc. v. Am. Heritage Prod., Inc., 694 F.2d 674, 677–80 (11th Cir. 1983) (incorporating Supreme Court of Georgia certified question holding that the right of publicity extends to "public figures who are [not] public officials" in the sense of holding public office); N.Y. Magazine v. Metro. Transit Auth., 987 F. Supp. 254, 260–69 (S.D.N.Y. 1997) (holding that defendant transit authority could not use refusal to violate right of publicity statute to defend against exclusion of advertisements that depicted Mayor Rudolph Giuliani in a less than complimentary light, and that an attempt to prevent display of the advertisements on public buses in New York City was an infringement of the magazine's First Amendment rights to political commentary "of public interest," notwithstanding that it was commercial speech).

[141] *See* Tyler Ochoa, *The Schwarzenegger Bobblehead Case: Introduction and Statement of Facts*, 45 SANTA CLARA L. REV. 547, 547 (2005).

the case was settled, it raised many legal and policy issues as to the application of the right of publicity to politicians as opposed to people whose celebrity is derived from other means.[142]

The issue was particularly confusing in the Governor Schwarzenegger situation because he had attained fame and celebrity through sports, film, and political careers.[143] Had the matter been judicially decided, the court may have had to decide specifically whether the defendant's dolls were commenting on the Governor's political persona—in which case they may have been protected by the First Amendment—or whether they could be seen as purely usurping the Governor's commercial interests in his persona and likeness.[144]

In the course of debates over the Schwarzenegger bobblehead dolls, commentators noted how few right-of-publicity actions had been brought by sitting politicians in the past.[145] Various suggestions were

---

[142] *See id.*

[143] *See id.* at 548–49.

[144] William T. Gallagher, *Strategic Intellectual Property Litigation, the Right of Publicity, and the Attenuation of Free Speech: Lessons from the Schwarzenegger Bobblehead Doll War (and Peace)*, 45 SANTA CLARA L. REV. 581, 597–98 (2005) ("[T]he Schwarzenegger likeness was not being used to sell other products but was the product itself, albeit in a creative expression of that image. The Schwarzenegger image was thus part of the 'raw materials' or the medium that the bobblehead doll's creators used to convey the multivocal messages the doll communicated. This message invariably comments, at least in part, on the Schwarzenegger political image and persona even if it also simultaneously comments on the Schwarzenegger Hollywood movie star persona. The governor himself, after all, has certainly made effective use of his Hollywood tough-guy, 'Terminator' image in political life. Schwarzenegger, now the governor, has become the 'Governator,' a play on words that evokes the dual personas of the current Schwarzenegger image. This image is also used extensively in political cartoons commenting on Schwarzenegger's new status as a politician. It would be disturbing for a court to hold that the right of publicity should trump the . . . defendants' right to sell a doll that similarly comments on the Schwarzenegger image. Such a decision would also be incongruous because it would permit Schwarzenegger to monopolize his image as the 'Governator' for both political and private profit."); Charles Harder & Henry Self III, *Schwarzenegger vs. Bobbleheads: The Case for Schwarzenegger*, 45 SANTA CLARA L. REV. 557, 563–64 (2005) (noting that there is a public affairs exception to the right of publicity in California, but that it would not likely apply to the Schwarzenegger bobblehead dolls because they contained no discernable political slogans or messages, but were merely a depiction or imitation of Schwarzenegger in the form of a doll).

[145] Gallagher, *supra* note 144, at 582 ("[I]t was virtually unprecedented for a sitting politician to sue in order to control the use of his or her image in similar circumstances [to the Schwarzenegger litigation]. The . . . defendants sold an entire series of bobbleheads depicting both living and deceased politicians; yet they had never previously been subject to legal threats or proceedings to prevent the sales of these dolls. In fact, as many news reports gleefully explained the [defendants] had previously sent copies of dolls to several politicians who apparently appreciated (or, perhaps, acquiesced to) having their likenesses made into a bobblehead doll."); Harder & Self, *supra* note 144, at 567 ("Few

raised as to why this might be the case, including: (a) politicians are often not generally concerned with commercial use of their image because "it is not their typical business,"[146] (b) politicians do not wish to invest resources into such claims,[147] (c) politicians want to avoid negative publicity that may arise from such claims[148] partly because they do not want to appear "humorless or soft-skinned,"[149] and (d) politicians are aware that the sale of products bearing their name or likeness might be protected by the First Amendment.[150]

A number of arguments may be raised in favor of extending the right of publicity to politicians and other public figures who are not celebrities in the sports and entertainment context. Surprisingly, there are very few obvious arguments as to why politicians should not enjoy a right of publicity in jurisdictions where the action is available. First Amendment concerns can be dealt with as a question of fact in an individual case—as suggested in comments on the Schwarzenegger bobblehead litigation.[151] Additionally, many politicians have been, and will likely continue to be, deterred from bringing right-of-publicity actions because of concerns about public perception and perhaps by concern for lack of success on First Amendment grounds.[152]

---

courts have had an opportunity to rule on an unauthorized commercial use of a political figure's name or likeness. Politicians do not typically pursue such claims . . . .").

[146] Harder & Self, *supra* note 144, at 567–68.

[147] *Id.* at 568.

[148] *Id.*

[149] Gallagher, *supra* note 144, at 583.

[150] *See id.*

[151] *Id.* at 597–98; Harder & Self, *supra* note 144, at 563–65 (noting that there is a public affairs exception to the right of publicity in California, but that it would not likely apply to the Schwarzenegger bobblehead dolls because they contained no discernable political slogans or messages, but were merely a depiction or imitation of Schwarzenegger in the form of a doll). Even prior to the Schwarzenegger bobblehead doll controversy, suggestions had been made that it would not be an impossible task to differentiate free speech concerns from purely commercial concerns in many right of publicity cases involving political figures. *See* Eileen Rielly, Note, *The Right of Publicity for Political Figures:* Martin Luther King, Jr., Center for Social Change, Inc. v. American Heritage Products, 46 U. PITT. L. REV. 1161, 1174 (1985) ("Where no legitimate first amendment purpose is served by the product, the manufacturer or advertiser should be required to pay for the privilege of using the political figure's name or face to sell it. As an example, even though commemorative items may deserve protection in some instances, it is hard to image [sic] that such items as 'plastic toy pencil sharpeners, soap products, target games, candy dispensers and beverage stirring rods' are a form of expression. An advertiser should not be able to hide behind the first amendment simply because he has chosen to exploit a political figure.").

[152] *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 346 (1995) ("'Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution. The First Amendment affords the broadest protection to such political expression in order to assure [the] unfet-

The arguments in favor of extending the right of publicity to politicians include the fact that, in cases of pure commercial use of a politician's name or likeness, there seems to be no good policy reason for differentiating between politicians and other public figures, like sports and entertainment stars.[153] Assuming that First Amendment concerns can effectively be dealt with on a case-by-case basis,[154] there seems to be no good policy reason why politicians who have spent time and effort developing their images should not be protected from unauthorized *commercial*, as opposed to political, exploitations of those images.[155] This would appear to be the case whatever the theoretical basis for the right of publicity—which is still a matter of some debate even in traditional celebrity-focused right-of-publicity cases.[156]

From a theoretical perspective, if the right of publicity is based on Lockean notions of property,[157] there are good arguments that political figures are just as deserving of reaping the rewards of their labors in developing their public personas as are celebrities.[158] If the right is based on an associated tort-based concept of unjust enrich-

---

tered interchange of ideas for the bringing about of political and social changes desired by the people.'" (quoting Roth v. United States, 354 U.S. 476, 484 (1957))) (internal quotation omitted).

[153] Harder & Self, *supra* note 144, at 565 ("The notion that political figures have no right to control the commercial use of their names and images contradicts both the letter and purpose of right of publicity laws. If the law did not apply to political figures, companies could freely exploit politicians' names and images in advertising for their products, or on the products themselves, with impunity. George W. Bush toothbrushes and Dick Cheney laundry detergent, for example, could pervade our supermarkets and households.").

[154] Gallagher, *supra* note 144, at 597–98; Harder & Self, *supra* note 144, at 562–64 (noting public affairs exception); *see also* Rielly, *supra* note 151, at 1174.

[155] Rielly, *supra* note 151, at 1170 (noting politicians' labor invested in public image similar to that of entertainers).

[156] *See* Dogan & Lemley, *supra* note 48, at 1180–90 (describing existing theoretical arguments to support the right to publicity and advocating for trademark-based justification); Madow, *supra* note 128, at 353–61 (describing moral, economic, and consumer protection-focused theories underlying the right of publicity); McKenna, *supra* note 48, at 245–84 (critiquing existing theories and offering right to self-definition as justification).

[157] Uhlaender v. Henricksen, 316 F. Supp. 1277, 1282 (D. Minn. 1970) ("It is this court's view that a celebrity has a legitimate proprietary interest in his public personality. A celebrity must be considered to have invested his years of practice and competition in a public personality which eventually may reach marketable status. That identity, embodied in his name, likeness . . . and other personal characteristics, is the fruit of his labors and is a type of property."). Some have critiqued the application of this theory in the right of publicity context. *See* Madow, *supra* note 128, at 354–55; *Winterland*, 210 U.S.P.Q. at 9 (describing right of publicity as property right); *see also* JOHN LOCKE, CONCERNING CIVIL GOVERNMENT, SECOND ESSAY: AN ESSAY CONCERNING THE TRUE ORIGINAL EXTENT AND END OF CIVIL GOVERNMENT (1690), *reprinted in* 35 GREAT BOOKS OF THE WESTERN WORLD 30 (Encyclopedia Britannica 1952) (describing notion of labor theory of property).

[158] Rielly, *supra* note 151, at 1170.

ment,[159] there is equally no reason why a person who has not shared in investing in the market value of a politician's image should be entitled to reap the economic rewards of the politician's efforts: "No social purpose is served by having the defendant get free some aspect of the plaintiff that would have market value and for which he would normally pay."[160] Even from the perspective that the right of publicity is grounded in theories of personal privacy, the right of publicity clearly protects some economic benefits.[161] Certainly, political cybersquatters are contemplating economic benefits when registering domain names corresponding to politicians' names.

Another reason why the right of publicity should be extended to politicians is that failure to do so might result in politicians being unable to make a living after devoting an often significant part of their lives, resources, and interests to public service. Many politicians will not try to make money from their names while they are in office,[162] although some may try to make money from their names and positions to fund a campaign for office.[163] Assuming that most politicians will not make a commercial profit from their personas during the majority of their political tenure, should they be potentially robbed of the commercial benefits of their names and images after they leave office?[164]

---

[159] Madow, *supra* note 128, at 355–56 (describing the case for and against an unjust-enrichment model for the right of publicity).

[160] Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 576 (1977) (quoting Harry Kalven, Jr., *Privacy in Tort Law—Were Warren & Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 331 (1966)).

[161] *See* GILSON LALONDE ET AL., *supra* note 18, § 2.16[5] (discussing the distinction between personal and property theories underlying the right of publicity and the relationship of personal remedies to proprietary remedies); Rielly, *supra* note 151, at 1164–66 (describing the evolution of the publicity right to a Lockean property right from a privacy intrusion tort); *see also* Madow, *supra* note 128, at 360–61 (describing personal autonomy theories that might explain the right of publicity in terms of personal *freedom*, rather than personal *property*); McKenna, *supra* note 48, at 290 (discussing economic damages for unauthorized endorsements).

[162] Rielly, *supra* note 151, at 1171 ("Most public servants are not trying to make money from their names while they are in office.").

[163] For example, Senator Hillary Clinton has obviously used her "celebrity" in publishing several books that may not otherwise have been published, and this money can be used to fund a presidential campaign. The authorship of these books was noted in the "hillaryclinton.com" domain name dispute as the basis for common law trademark rights in Senator Clinton's name. *Clinton*, No. FA0502000414641.

[164] Rielly, *supra* note 151, at 1171 ("[Public servants] may . . . wish to market themselves for profit after they leave office. The decision to enter the political arena should not forever foreclose a person from realizing the financial benefits of fame. If a political figure has no control over the commercial use of his name and face until he retires, he may not ever be able to realize any financial benefits from it. For a political figure to exercise the right himself while in office would not likely be viewed favorably by the public and, if he

In the electoral context, political cybersquatting activities may prevent political speech in the lead-up to an election, which is clearly an undesirable and wasteful social outcome. It is difficult to imagine that political cybersquatting could result in *more* or *more useful* political discourse pertaining to a politician in the lead-up to an election. Thus, political discourse is ultimately made more expensive by this conduct. The use of the name in the political context in the absence of the cybersquatting conduct would be much less expensive than if a cybersquatter first needs to be paid off to secure the use of the name in the electoral context.[165] The cybersquatter's socially wasteful commercial interests could limit a candidate's otherwise protected First Amendment speech in the absence of some remedy for the politician.[166] It may be that the right of publicity is a plausible legal avenue to address such conduct.[167] If indeed there is no reason not to extend the right to politicians, at least in contexts where the defendant's use of a politician's name or likeness is for purely commercial purposes, then there should be no objection to developing the right of publicity in this context.[168]

---

cannot prevent others from exploiting his fame, he will have little ability to market himself when he retires.").

[165] *See* Friess, *supra* note 9 (discussing desire of political domain name cybersquatters to profit from the names while noting that domain names are inexpensive to register).

[166] It is also possible that if the politician does not want to use the domain name, the interests of cybersquatters should be secondary to interests in the name by other people who want to use the name for actual political discourse in the context of the election as opposed to commercial profit. However, in this Article it is contemplated that politicians will generally want to hold registrations of domain names that most closely resemble their own names in the electoral context.

[167] *See* Harder & Self, *supra* note 144, at 565–67. Nevertheless, at least one court has found that First Amendment concerns about limiting political speech may override the right of publicity for a politician where the website in question was critical of the politician. *See* Ficker v. Tuohy, 305 F. Supp. 2d 569, 570–72 (D. Md. 2004) (denying temporary injunction including a count of right of publicity where political critic used the politician's name as the domain name for a site critical of the politician, but which stated that the site was not affiliated with the politician and included a link to his actual website); *see also* Herbert v. Okla. Christian Coal., 992 P.2d 322, 332 (Okla. 1999) (holding that defendant's voter guide falsely stating plaintiff candidate's position did not rise to actual malice in defamation action and could not be submitted to the jury).

[168] Additionally, in cases where the defendant's use of the politician's name is purely for commercial profit with respect to the sale of goods or services, an action for trademark infringement may also be possible whether or not the politician has registered her name as a trademark. *See* 15 U.S.C. § 1125(a)(1) (2000). Section 1125(a)(1) may well protect an unregistered trademark in this context. In fact, Professors Dogan and Lemley have suggested that the right of publicity could be practically abolished because most relevant conduct is now covered by basic trademark principles. Dogan & Lemley, *supra* note 48, at 1212–13.

There may be some question as to whether the right of publicity provides appropriate remedies for political cybersquatting. Generally in a traditional right-of-publicity case, a plaintiff will want an injunction[169] to prevent the sale of the products in question as well as perhaps an account of profits[170] or some other kind of monetary damages.[171] In the political cybersquatting case, the politician in question will more than likely want transfer of the name to her rather than an injunction or monetary compensation. Thus, the remedies for actions in the right of publicity are not as good a fit for political cybersquatting as, say, the UDRP remedy of transfer of the name from a bad faith registrant to a person with a legitimate interest in the name.[172] Because the UDRP is cheap, efficient, and global in its scope, and because its remedies are of the kind most suited to political cybersquatting, it may be more sensible at least in the short term to extend the UDRP to political cybersquatting than to rely on the right of publicity.[173]

In summary, it is simply not clear whether, or to what extent, the right of publicity might help potential politician-plaintiffs in a cybersquatting action, at least as currently framed.[174] The right of publicity may be a useful avenue of development for future law and policy, but at the moment it contains many uncertainties, including: (a) lack of domestic and international harmonization as to the contours of the right of publicity, (b) uncertainty as to the scope of the right in the context of domain names reflecting politicians' names,[175] and (c) questions as to whether the kind of remedies tailored for the right of

---

[169] *See* GILSON LALONDE ET AL., *supra* note 18, § 2.16[6] (stating that courts almost always grant injunctions in successful right of publicity actions, because "the primary purpose of the right of publicity is to prevent the unauthorized use of a person's name and likeness").

[170] *Id.* ("The more common measure of damages in right of publicity cases is the commercial or fair market value of the endorsement. Other losses may also be included, such as a decrease in the manufacturer's sales of a competing product properly endorsed by the celebrity, and an accounting for profits may be awarded.").

[171] *Id.* (noting that outside of economic damages, general damages may be awarded for "hurt feelings," and that punitive damages may occasionally be awarded where the common law element of malicious intent can be established).

[172] *See supra* notes 44–46 and accompanying text.

[173] *See* InterNIC FAQs, *supra* note 44; UDRP Rules, *supra* note 46, ¶¶ 3, 5, 15, 16.

[174] Even Professors Dogan and Lemley, both of whom question the need for a right of publicity in light of the fact that trademark law can protect certain personal interests in relevant domain names, only refer to "celebrity" domain names, and their cited examples do not include political cybersquatting. *See* Dogan & Lemley, *supra* note 48, at 1203.

[175] *See, e.g.*, *Friends of Kathleen Kennedy Townsend*, No. D2002-0451, ¶ 6 (suggesting politician Townsend would not have a common law trademark in her personal name used for purely political purposes).

publicity are really what a plaintiff will want in a political cybersquatting case.[176] Similar problems may arise in relation to other *sui generis* state law initiatives that might protect politicians against political cybersquatters. An obvious example may be found in recently developed provisions of California's Business and Professions Code.

3. California's Business and Professions Code Section 17525

California's Business and Professions Code was revised soon after the enactment of the ACPA to deal with certain kinds of cybersquatting activities.[177] In August of 2000, the California legislature enacted several new sections of the Code to counter these kinds of activities—with a somewhat broader scope than the federal legislation.[178] The new subsection 17525(a) of the Code provides:

> It is unlawful for a person, with a bad faith intent to register, traffic in, or use a domain name, that is identical or confusingly similar to the personal name of another living person or deceased personality, without regard to the goods or services of the parties.[179]

This prohibition is broader than the personal name provisions of the ACPA in two respects.[180] The first is that it extends protection to deceased as well as living persons.[181] The second, and more relevant for the purposes of this Article, is that the California legislation sets out a list of bad faith factors that are somewhat broader than those in the federal legislation.[182] In particular, subsection 17526(j) of the California legislation includes as a bad faith factor "[t]he intent of a person

---

[176] *See* GILSON LALONDE ET AL., *supra* note 18, § 2.16[6] (discussing remedies applicable in right of publicity actions).

[177] CAL. BUS. & PROF. CODE §§ 17525–17526 (West 1997 & Supp. 2007).

[178] *Compare* 15 U.S.C.A. §§ 1125(d), 1129 (West 1998 & Supp. 2007), *with* CAL. BUS. & PROF. CODE §§ 17525–17526.

[179] CAL. BUS. & PROF. CODE § 17525(a).

[180] *Compare* 15 U.S.C.A. § 1129(1)(A), *with* CAL. BUS. & PROF. CODE § 17525.

[181] CAL. BUS. & PROF. CODE §§ 17525–17526.

[182] *See id.* § 17526. The federal legislation's "bad faith" factors technically do not apply specifically to 15 U.S.C. § 1129(1)(A), as they are in the provision dealing with cybersquatting relating to trademarks (as opposed to personal names). 15 U.S.C.A. § 1125(d)(1)(B)(i). However, those factors may well assist courts in interpreting § 1129 as there is no specific guidance as to interpreting the intent requirement in § 1129. *See id.* § 1129. Note, however, that § 1129 does not specifically contain a "bad faith" requirement beyond the profit-seeking intent. *See id.*

alleged to be in violation of this article to mislead, deceive, or defraud voters."[183]

At first glance, this legislation appears to have some application to political cybersquatting in the sense that the registrant in question has registered a domain name that corresponds to the name of a living person without regard to the goods or services of the parties.[184] But the real question here would be whether the registrant had an intent to "mislead, deceive, or defraud voters."[185] A political cybersquatter who is not using the domain name to promulgate any message about the relevant politician, other than that the domain name is available for sale, probably has not engaged in such conduct.[186] Unlike a person engaging in political *cyberfraud*,[187] by definition, a political cybersquatter is trying to make a profit from the registration of the name without actually disseminating any particular message to voters.

It is possible that a political cybersquatter might be found to have violated subsection 17525(a) regardless of a failure to satisfy the voter deception bad faith test in subsection 17526(j) on a variety of other grounds.[188] It is important to recognize that the bad faith factors in section 17526 are not intended to be exclusive.[189] Additionally, some of the other bad faith factors in section 17526 may apply to political cybersquatting although not, perhaps, as obviously at first glance as subsection 17526(j) because they do not focus specifically on the political context. They include:

> (e) The intent of a person . . . to divert consumers from the person's . . . online location to a site accessible under the domain name that could harm the goodwill represented by the person's . . . name either for commercial gain or with the intent to tarnish or disparage the person's . . . name by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site.
> (f) The offer by a person alleged to be in violation of this article to transfer, sell, or otherwise assign the domain name to

---

[183] CAL. BUS. & PROF. CODE § 17526(j).

[184] *See id.* § 17525(a).

[185] *See id.* § 17526(j).

[186] *See id.*

[187] *See infra* notes 235–238 and accompanying text.

[188] CAL. BUS. & PROF. CODE § 17526.

[189] *Id.* The wording of § 17526 itself makes this clear by stating, "In determining whether there is a bad faith intent pursuant to Section 17525, a court may consider factors, including, but not limited to, the following . . . ." *Id.* The list of bad faith factors follows. *Id.*

> the rightful owner or any third party for substantial consideration without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services.
>
> . . . .
>
> (h) The registration or acquisition by the person alleged to be in violation of this article of multiple domain names that are identical or confusingly similar to names of other living persons or deceased personalities.
>
> (i) Whether the person alleged to be in violation of this article sought or obtained consent from the rightful owner to register, traffic in, or use the domain name.[190]

Subsections (e) and (f) are borrowed relatively directly from the policies and principles underlying both the ACPA and the UDRP.[191] Though they appear potentially to have some application to political cybersquatting, they both relate to trademark concepts: likelihood of confusion in the case of subsection (e)[192] and bona fide offering of goods or services in the case of subsection (f).[193] It may be that courts interpreting these provisions in the political cybersquatting context would take the view that these bad faith factors are related to situations akin to trademark infringement or traditional commercial cybersquatting and do not apply to political cybersquatting.[194]

---

[190] *Id.*

[191] *See* 15 U.S.C. § 1114(1)(a) (2000) (requiring consumer confusion for registered trademark infringement action); *id.* § 1125(a)(1)(A) (requiring consumer confusion for common law trademark infringement action); 15 U.S.C.A. § 1125(d)(1) (West 1998 & Supp. 2007) (prohibiting cybersquatting of trademark-based domain names); UDRP, *supra* note 14, ¶ 4(a)(i).

[192] CAL. BUS. & PROF. CODE § 17526; *see* 15 U.S.C. § 1114(1)(a) (requiring likelihood of consumer confusion or deception for registered trademark infringement action); *id.* § 1125(a)(1)(A) (requiring consumer confusion for common law trademark infringement action).

[193] CAL. BUS. & PROF. CODE § 17526; *see* 15 U.S.C. § 1114(1)(a) (requiring commercial exploitation of relevant goods or services for registered trademark infringement action); *id.* § 1125(a)(1)(A) (requiring commercial exploitation of relevant goods or services for common law trademark infringement action).

[194] *See* 15 U.S.C. § 1114(1)(a) (requiring commercial exploitation of relevant goods or services for registered trademark infringement action); *id.* § 1125(a)(1)(A); CAL. BUS. & PROF. CODE § 17526.

Subsection (h) is borrowed directly from the ACPA,[195] which in turn was drafted in response to cases where cybersquatters registered multiple domain names corresponding to well-known trademarks.[196] Whether it could apply to a political cybersquatting case depends on the circumstances. In fact, in both the commercial and political contexts, it is obviously possible for an alleged cybersquatter not to register multiple domain names, hoping instead to make a profit from the sale of just one particularly promising name.

Subsection (i) might be the most fruitful avenue for a politician concerned about political cybersquatting.[197] The one obvious problem with it is that it does not make clear who is a "rightful owner" of a relevant domain name and on what theoretical basis.[198] Modern trademark law appears to have assumed in many circumstances, including the ACPA, that a trademark holder is the "rightful owner" of a corresponding domain name, at least as against bad faith cybersquatters. It is possible that the same may not hold true for politicians who may or may not be able to trademark their personal names. On the other hand, if one takes the view that any form of cybersquatting, including political cybersquatting, is inherently socially and economically wasteful, then it might be easier to argue that a politician is the "rightful owner" of a corresponding domain name in this context. Thus, subsection 17526(i) might prove useful to politicians who are the victims of political cybersquatting, depending on how courts interpret the scope of this bad faith factor.[199]

The California Business and Professions Code provisions also raise an important practical problem in that the approach is untested state legislation that has not been adopted in other jurisdictions. It may serve as a useful "legislative laboratory"[200] on many issues related

---

[195] *See* 15 U.S.C.A. § 1125(d)(1)(B)(i)(VIII) (West 1998 & Supp. 2007) (contemplating as a "bad faith factor" under the trademark-based provisions of the ACPA, the defendant'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 such domain names, without regard to the goods or services of the parties . . . ."); CAL. BUS. & PROF. CODE § 17526(h).

[196] The conduct of Mr. Dennis Toeppen in the early days of Internet domain name disputes is one such example. *See Panavision*, 141 F.3d at 1319; Lipton, *supra* note 10, at 1370–71.

[197] *See* CAL. BUS. & PROF. CODE § 17526(i).

[198] *See id.*

[199] *See id.*

[200] U.S. PATENT & TRADEMARK OFFICE, REPORT TO CONGRESS: THE ANTICYBERSQUATTING CONSUMER PROTECTION ACT OF 1999, SECTION 3006 CONCERNING THE ABUSIVE REGIS-

to cybersquatting, but it may not yet be of much assistance to politicians concerned about this conduct.

E. *Political Cybersquatting: Possible Solutions*

There are obviously various different avenues that politicians concerned about political cybersquatting can pursue, depending on the context of the relevant conduct and jurisdiction. If, for example, a politician can establish trademark rights in her name, like Senator Clinton has done,[201] she will have more options for reprisal against a cybersquatter, as she might avail herself of the trademark-based provisions of the ACPA[202] or the UDRP,[203] as well as some of the other remedies discussed in the preceding sections.[204] She might also be able to mount a traditional trademark infringement action if she can establish the requisite elements for such an action, including likelihood of consumer confusion as to her sponsorship or affiliation with particular goods or services or commercial activities.[205] In the absence of a trademark action, other remedies might be available, such as those arising under the "personal name" provisions of the ACPA,[206] as well as potential actions under the right-of-publicity or various state legislation, if available.[207]

The main problem with the current legal framework is that it is piecemeal and quite context-specific with respect to political cybersquatting. Much will depend on factors such as the jurisdiction in which the politician and registrant are located or the domain name was registered, as well as on whether the politician can establish a trademark right in her name.[208] Additionally, the system is not nationally or globally harmonized in a way that effectively deals with a problem that often has national or global dimensions.[209] Particularly in the context of a

---

TRATION OF DOMAIN NAMES 5, *available at* http://www.uspto.gov/web/offices/dcom/olia/tmcybpiracy/repcongress.pdf (last visited Oct. 15, 2007) ("California may serve as a legislative 'laboratory' on [the issue of use of personal names in domain names].").

[201] *Clinton*, No. FA0502000414641 (finding that Senator Clinton established common law rights in the mark "Hillary Clinton").

[202] 15 U.S.C.A. § 1125(d)(1) (West 1998 & Supp. 2007).

[203] UDRP, *supra* note 14 ¶ 4(a)(i).

[204] *See supra* notes 95–200 and accompanying text.

[205] 15 U.S.C. § 1125(a) (2000).

[206] *Id.* § 1129.

[207] *See* CAL. BUS. & PROF. CODE § 17525(a) (West 1997 & Supp. 2007); CAL. ELEC. CODE §§ 18320 (West 2003 & Supp. 2007).

[208] *See supra* notes 78–88, 119–123 and accompanying text.

[209] For example, Senator Obama, a national candidate, owns barackobama.com, but obama.com appears to be registered to an individual of that name in Japan. *See* Whois.net, *supra* note 68.

presidential election, people all around the United States and in other countries may want to register domain names corresponding to potential candidates' names with an intent to seek profit from the sale of the names.[210] These uses may or may not technically amount to trademark infringements, depending on whether the politician in question has trademark rights in her name—either registered or common law rights—and whether the cybersquatting conduct fits the legal notion of a trademark infringement.[211] Additionally, these uses may or may not run afoul of any of the other laws described earlier.[212]

Whatever the view one takes of cybersquatting generally, political cybersquatting in particular clearly adds costs to an electoral system without providing any specific benefits. Creating markets for valuable political domain names and effectively holding the names hostage awaiting the highest bidder can be wasteful, particularly in the time-sensitive electoral context. If financial gain is the only purpose of the conduct—as opposed to facilitating political speech in some way—it should be proscribed.

One obvious answer to this problem and to some other associated problems, would be to ban legislatively *all* forms of cybersquatting, political or otherwise. In other words, a general rule could be adopted on the national or international level prohibiting all registrations of domain names where the intent is to profit from selling the name rather than to accomplish a legitimate use or purpose such as facilitating First Amendment speech. Although adopting this rule would overlap with the current trademark-based regulations, such overlap does not present a problem.[213] This type of blanket rule would prohibit political cybersquatting as well as other conduct that wastes a potentially valuable resource, political or otherwise.[214] Alternatively, one could do the same

---

[210] *See* Friess, *supra* note 9.

[211] *See* 15 U.S.C. § 1125(a).

[212] *See supra* notes 95–200 and accompanying text.

[213] *See* 15 U.S.C.A. § 1125(d)(1) (West 1998 & Supp. 2007); UDRP, *supra* note 14, ¶ 4(a).

[214] A good example of such alternate conduct would be conduct that might be termed "anticipatory cybersquatting"—where a registrant registers multiple domain names that do not necessarily correspond to trademarks or personal names, but rather correspond to general ideas that may be valuable in a particular field of commerce. For example, a registrant might register multiple variations of the word "sports," "cars," or "movies" in a domain name—say, "cars.com," "motorcars.com," "carworld.com," and "caruniverse.com." If the registrant registers enough of these variations, she could effectively preempt anyone who wanted to register a domain name to sell cars and hold relevant domain names for ransom for an exorbitant fee. This would mean that the person wanting to enter the field could have to pay hundreds, thousands, or even millions of dollars for a relevant domain name instead of the standard registration fee of ten to twenty dollars.

thing with respect only to political cybersquatting, depending on the willingness of relevant regulatory bodies to legislate more or less broadly on the question.[215]

One problem with establishing such legal rules—either generally applicable, or specific to the political situation—is precisely how they should be enacted and enforced. This is not necessarily a new question. It has already been confronted by the drafters of the ACPA and the UDRP, not to mention the various California statutes described above.[216] Legislation dealing outside the trademark context, however, either with politicians' names, or with cybersquatting generally, may raise some new issues.

A purely domestic solution would require either federal legislation or uniform state legislation. The downside of federal legislation is establishing which constitutional head of legislative power would support such a regulation.[217] Perhaps the Commerce Clause power[218] could justify such rules on the basis that the conduct in question potentially affects communications and commerce[219] across all states. However, federal legislation would not necessarily deter cybersquatters outside the United States from engaging in this conduct. It is cheap and easy to register a domain name, even a ".com" domain name, in many countries.[220] Thus, a federal legislative package would require a jurisdictional provision like the "in rem" provisions in the ACPA to ensure its effective enforcement.[221] State legislation, on the other hand, would not raise the federal legislative power questions

---

[215] *See* CAL. ELEC. CODE § 18320 (West 2003 & Supp. 2007) (limiting the PCAA to ballot measure websites).

[216] CAL. BUS. & PROF. CODE § 17525(a) (West 1997 & Supp. 2007); CAL. ELEC. CODE §§ 18320–18323 (West 2003 & Supp. 2007).

[217] *See generally* U.S. CONST. art. I.

[218] *Id.* art I, § 8, cl. 3 (stating that Congress shall have the power "[t]o regulate Commerce with foreign Nations, and among the several States").

[219] *See Bucci*, 42 U.S.P.Q.2d (BNA) at 1434–35 (interpreting the application of the Lanham Act to a domain name dispute and noting that, as a statute whose Congressional jurisdiction is based on the commerce power, the Lanham Act applies to Internet domain name registrations and uses because they are part of interstate commerce on two grounds: first, websites can provide commercial and informational services in multiple states, and second, Internet users constitute a national and international audience who must use interstate telephone lines to access the Internet).

[220] *See* InterNIC, The Accredited Registrar Directory: Registrars Alphabetical by Origin, http://www.internic.net/origin.html (last visited Oct. 15, 2007) (listing global domain name registries accredited by ICANN and stating it was last updated September 7, 2007).

[221] 15 U.S.C.A. § 1125(d)(2)(A)(ii) (West 1998 & Supp. 2007) (providing that a plaintiff may proceed against a domain name on an in rem jurisdictional basis if personal jurisdiction cannot be effectively established against the relevant domain name registrant).

but would raise difficulties of creating a statute on which state legislatures could substantially agree. It may also raise jurisdictional concerns and require in rem provisions to cover domain name registrants situated outside the relevant jurisdiction.[222]

An alternative, and perhaps more obvious solution, would be to add specific personal name protections to the UDRP.[223] In other words, where the UDRP is currently limited to protecting trademark-based rights from cybersquatting,[224] it could be extended to protect personal names against cybersquatting regardless of whether any particular name might be accepted as a registered or common law trademark.[225] The changes could be limited to politicians' names or could extend more broadly to celebrities and other public figures. The broader approach would certainly cover some difficult situations that have arisen to date under the UDRP.[226] However, the narrower approach, one focused purely on politicians' names, might be simpler and less contentious at least in the short term. This is because of the fundamental importance to the democratic process of free and accurate information about politicians, particularly in the lead-up to an election. Celebrities presumably have less trouble than politicians under the UDRP as currently drafted.[227] This is because celebrities are more likely than politicians to be able to establish trademark-like rights in their names, given that their names and images are used predominantly for commercial purposes.[228] A politician who wants to avoid commercialization of his image may thus currently be disadvantaged under the UDRP.[229] The same may be said of a less "famous"

---

[222] *See id.* § 1125(d)(2).

[223] *See* UDRP, *supra* note 14, ¶ 4(a).

[224] *Id.* ¶ 4(a)(i) (requiring complainant to establish trademark interest as a requisite element of a UDRP claim).

[225] *See id.* This change was considered; but ultimately rejected, in the second WIPO report on the domain name process. *See* WIPO SECOND DOMAIN PROCESS, *supra* note 89, ¶¶ 189–204.

[226] These difficult situations include the case of celebrities who are undoubtedly well known but who have been found not necessarily to hold common law trademark rights in their personal names. *See, e.g.*, *Springsteen*, No. D2000-1532, ¶ 6 (stating it was "by no means clear" that Bruce Springsteen's name was protectible under common law trademark rights enforceable under the UDRP but deciding the case on other grounds).

[227] *Compare Roberts*, No. D2000-0210, ¶ 6, *with Townsend*, No. D2002-0030, ¶ 6 (failing to protect politician Kathleen Kennedy Townsend's name under the UDRP). *But see Clinton*, No. FA0502000414641.

[228] *Compare Roberts*, No. D2000-0210, ¶ 6, *with Townsend*, No. D2002-0030, ¶ 6. *But see Clinton*, No. FA0502000414641 (holding Hillary Clinton had established a trademark interest in her name in part because of her book sales).

[229] *Compare Townsend*, No. D2002-0030, ¶ 6, *with Clinton*, No. FA0502000414641.

politician who has not yet established a major public persona.[230] An extension of the UDRP rules to cover politicians' personal names as such could correct these imbalances in the system.[231]

The advantages of this approach over federal and state legislation are many. The UDRP procedures are fast, inexpensive, and international in scope.[232] The remedies available under the UDRP are precisely the kinds of remedies a politician will want in a political cybersquatting case—an arbitral order that the domain name in question be transferred to the politician.[233] The addition of a "politician's name protection" provision to the UDRP would be a minor drafting change and could be achieved relatively quickly and simply.[234]

II. Political Cyberfraud

A. *Distinguishing Cyberfraud from Cybersquatting*

Political cyberfraud, as defined in this Article, includes various categories of bad faith content involving registration of a domain name corresponding to a politician's name.[235] It differs from *political cybersquatting* in that it looks to the substantive content of the relevant website in association with the domain name, unlike cybersquatting, which reflects a simple attempt to sell the domain name.[236] Examples of cyberfraud would include publishing misleading or damaging information on a website about the relevant politician or a fraudulently attempting to raise funds in the name of the politician under a domain name corresponding to the politician's name.[237] The substantive content itself of a relevant website may be either legitimate, such as bona fide political commentary, or illegitimate, such as defamatory remarks.

---

[230] *Compare Townsend*, No. D2002-0030, ¶ 6, *with Clinton*, No. FA0502000414641.

[231] *Compare Townsend*, No. D2002-0030, ¶ 6, *with Clinton*, No. FA0502000414641.

[232] *See* UDRP Rules, *supra* note 46, ¶¶ 3, 5, 15, 16; *supra* notes 44–46 and accompanying text.

[233] *See* UDRP, *supra* note 14, ¶ 4(i); *see also Clinton*, No. FA0502000414641.

[234] Nevertheless, although the change itself would not be complicated, the WIPO Second Domain Name Process would seem to suggest that this is contentious. *See supra* note 90.

[235] *See* Cal. Bus. & Prof. Code §§ 17525–17526 (West 1997 & Supp. 2007) (prohibiting and defining certain types of cyberfraud).

[236] *See* Nathenson, *supra* note 15, at 925–26; *see also* Dictionary.com, http://dictionary.reference.com/browse/cybersquatting (last visited Oct. 12, 2007) (defining cybersquatting as "the registration of a commercially valuable Internet domain name, as a trademark, with the intention of selling it or profiting from its use").

[237] *See* Cal. Elec. Code § 18320(c)(1) (West 2003 & Supp. 2007) (defining political cyberfraud).

But cyberfraud is concerned with publishing the content in concert with a domain name corresponding to a politician's name in a manner that appears to cloak the speech with a misleading sense of authority or truthfulness.[238]

This assumes, of course, that Internet users would expect that a domain name such as, say, "ralphnader.com" would resolve to a website actually authorized, sponsored, or maintained by Ralph Nader. In some ways, this assumption parallels presumptions that appear to be developing in commercial trademark law with respect to domain names corresponding to well-known trademarks.[239] There is now some authority that "trademark.com" names should resolve to websites authorized or sponsored by relevant trademark holders.[240]

A domain name registrant committing "cyberfraud" may or may not have an additional purpose to sell the domain name, but cyberfraud and cybersquatting are treated differently in this Article for a number of reasons. Cyberfraud will obviously raise more difficult issues of subjective judgment than cybersquatting because when the focus turns to evaluating the substantive content of a website, more difficult interpretive questions will arise than in cases of pure waste of a domain name resource.[241] This is why, in many ways, pure cybersquatting will be much easier to regulate than cyberfraud. Regulating cybersquatting will likely be much less contentious because it would simply preserve available forums for political debate and prevent wasting of those resources, particularly during elections. Regulating cyberfraud, on the other hand, might involve promoting certain kinds of political speech above other kinds of political speech in an electoral context. Not only might these questions be much more subjective than questions involving pure cybersquatting, but their resolutions might differ from jurisdiction to jurisdiction and from culture to culture. Thus, regulation should probably be as minimally invasive of speech as possible.[242] Moreover, these issues might lend themselves

---

[238] *See id.*

[239] *See* 15 U.S.C.A. § 1125(d) (West 1998 & Supp. 2007).

[240] *See id.*

[241] *See supra* notes 235–238 and accompanying text (defining political cyberfraud to include misleading or fraudulent substantive content).

[242] *See* Ficker v. Tuohy, 305 F. Supp. 2d 569, 570–71 (D. Md. 2004) (denying temporary injunction sought under, *inter alia*, the ACPA, due in large part to First Amendment concerns, where political critic used the politician's name as the domain name for his website critical of the politician, but which stated that the site was not affiliated with the politician and included a link to his actual website).

more appropriately to local, rather than global, regulation, unlike cybersquatting.

Additionally, some aspects of conduct described here as cyberfraud may already be covered by relevant local laws and may not, in fact, need as much legislative or regulatory reform as pure political cybersquatting.[243] The promulgation of defamatory messages about a politician on a website regardless of the domain name used could be the subject of a defamation action under current law, though politicians, as public figures, would be subject to the heightened "actual malice standard."[244] Attempting to defraud the public and raise money fraudulently under a politician's name (and domain name) would presumably contravene various criminal statutes.[245] Of course, conduct like this arguably has two parts: one is the website's content and the other is the unauthorized use of a domain name corresponding to a politician's name.[246] It may be that current defamation and fraud laws cover much of the conduct relating to web content, but that it is necessary to create additional laws relating to the use of a domain name corresponding to a politician's name in the noncommercial context.[247]

---

[243] *See, e.g.*, Anderson v. Augusta Chronicle, 610 S.E.2d 428, 429–30, 433 (S.C. 2005) (allowing jury to reach question of whether false statement about political candidate was made with actual malice).

[244] *See* N.Y. Times v. Sullivan, 376 U.S. 254, 279–80 (1964) (establishing actual malice standard for public figure defamation plaintiffs); *see also* Monitor Patriot Co. v. Roy, 401 U.S. 265, 271–72 (1971) (applying *New York Times* standard to political candidates); Robert C. Berness, Note, *Norms of Judicial Behavior: Understanding Restrictions on Judicial Candidate Speech in the Age of Attack Politics*, 53 RUTGERS L. REV. 1027, 1061 n.207 (2001) (noting that the *New York Times* standard "made it exceedingly difficult for public figures, including political candidates, to succeed on defamation claims").

[245] The Federal Department of Justice has defined "Internet fraud" as follows: "The term 'Internet fraud' refers generally to any type of fraud scheme that uses one or more components of the Internet—such as chat rooms, e-mail, message boards, or Web sites—to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme." *See* Dep't of Justice, Internet Fraud, http://www.usdoj.gov/criminal/fraud/Internet (last visited Oct. 14, 2007). Although the Department of Justice does not appear to be actively focusing on political fraud at this time, it appears to be increasingly concerned with criminal prosecutions for Internet fraud generally. *See id.* (stating that the government has brought actions for Internet fraud in the areas of online auctions, business schemes, and credit cards, *inter alia*).

[246] *See* Press Release, Ky. Sec'y of State, Grayson Announces First in the Nation Online Service to Protect Voters (Sept. 27, 2005), *available at* http://www.kentucky.gov/Newsroom/sos/article19.htm (discussing state's plan to provide certification of candidate websites and online fundraising operations to protect voters from fraudulent schemes).

[247] *See* 15 U.S.C. § 1129 (2000) (covering personal names in the profit-seeking context); *Ficker*, 305 F. Supp. 2d at 572 (noting that the court was not convinced that the ACPA protected a "non-trademarked personal name, where the websites have no commercial use").

Registering a political domain name to mislead the public might be somewhat akin to the registration of a domain name corresponding to a trademark to promulgate a misleading or deceptive message about the trademark holder.[248] Such conduct has been variously dealt with under current trademark laws.[249] However, it raises additional dimensions in the political context because of the importance of free speech in political discourse.

Additionally, the theoretical basis underlying personal domain name regulation in the political context impacts the policy choices made. It is arguable that, as a theoretical matter, regulation of fraudulent conduct in the political context should not be based on the notion of a property-like right in a personal name as it is in the trademark context.[250] Although trademarks have clearly attained a property-like status within our legal system, it is not clear that politicians' names, or at least all politicians' names, have achieved a similar status.[251] Even just within the context of the right of publicity, it is not clear that politicians' names should be treated in the same way as celebrities' names because a celebrity's persona has often attained a trademark-like status corresponding to a property right, where a politician's name and likeness often has not.[252] Of course, the property-like value of a trademark is not surprising because trademarks are based largely on protecting commercial interests.[253] Thus, Senator Clinton, as a politician, has been

---

[248] *See* Joshua Quittner, *Billions Registered*, WIRED, Oct. 1994, http://www.wired.com/wired/archive/2.10/mcdonalds_pr.html (discussing registration by Princeton Review, a test prep company, of Kaplan.com, which corresponds to Princeton Review test-prep competitor Kaplan). Princeton Review used the Kaplan.com site to discuss reasons why it was superior to its competitor, and at the time, no law prohibited such use. *Id.*

[249] *See* 15 U.S.C. § 1114(1) (prohibiting infringement of registered trademarks); *id.* § 1125(a)(1) (prohibiting infringement of common law trademarks); 15 U.S.C.A. § 1125(d) (West 1998 & Supp. 2007) (prohibiting registration of domain names corresponding to trademarks).

[250] Trademarks are often colloquially referred to as "property" rights although technically they are not "property" in more traditional senses of the word. Stacey L. Dogan & Mark A. Lemley, *Trademarks and Consumer Search Costs on the Internet*, 41 HOUS. L. REV. 777, 788 (2004) (noting "trademarks are not property rights in gross, but limited entitlements to protect against uses that diminish the informative value of marks"); Mark A. Lemley, *The Modern Lanham Act and the Death of Common Sense*, 108 YALE L.J. 1687, 1687–88 (1999) ("Commentators and even courts increasingly talk about trademarks as property rights; as things valuable in and of themselves, rather than for the product goodwill they embody.").

[251] *See* Lemley, *supra* note 250, at 1687–88 (discussing view of trademarks as independently valuable property rights).

[252] As noted, a politician's public persona is usually based on activities in the public service realm rather than on commercial activities. *See supra* notes 162–164 and accompanying text.

[253] *See* GILSON LALONDE ET AL., *supra* note 18, § 1.03[1], [2].

found to have a common law trademark right in her name through a combination of her *commercial* and political activities.[254]

In the political context, the theoretical basis underlying the protection of a politician's name in a corresponding domain space more appropriately resides in notions of democratic government and free speech, rather than in notions of property as in the commercial context. Based on a speech-facilitating theory of regulation, it seems intuitive that at least the most obvious iterations of a politician's name should be protected in a domain space for that politician's own purposes.[255] In accordance with the underlying notion of democratic communication, this presumption is likely the most effective one for preserving and facilitating political debate, particularly in an electoral context. Furthermore, reserving the domain name probably accords with voter expectations that "politicianname.com" is sponsored by that politician and is likely the most effective presumption for preserving and facilitating political debate. But the reservation of the domain name—or at least "first rights" in the domain name—to the politician in question should not extend to blocking all iterations of that person's name in the domain space for legitimate political discussion purposes. In other words, if someone wanted to register "hillarysucks.com" for a website critical of Senator Clinton, that should be permitted so long as the more obvious versions of her name, such as "hillaryclinton.com," are reserved to Senator Clinton.

To this end, even if the theoretical basis underlying protection of a politician's name in the domain space is different from the theory behind protecting a trademark holder's interest in a domain name, the results should be similar. But the parallel result does not mean a politician's rights in her name should necessarily be equated to a property right. Rather, it is because the Internet is an important communications system and the domain name system is a significant method for users to navigate that system. These users probably have similar expectations regardless of the context. If the social expectations are that the "rightful" holder of the name is the politician in the political context or the trademark holder in the commercial context, it is possible to draw into the political context some principles that have been developed in the trademark context to date. Thus, the protection of social expecta-

---

[254] Clinton v. Dinoia a/k/a SZK.com, No. FA0502000414641 (NAF Mar. 18, 2005), http://www.arb-forum.com/domains/decisions/414641.htm (finding Clinton established common law trademark rights in the "Hillary Clinton" mark).

[255] *Cf.* 15 U.S.C.A. § 1125(d) (West 1998 & Supp. 2007) (prohibiting those who do not own trademarks from using domain names corresponding to others' trademarks).

tions in the domain space, whether those expectations are based on theories of representative democracy or commercial trademark law, should be a paramount concern of regulators in this area.

This appears to have been the case in the commercial trademark context where some courts seem to be developing a presumption in domain name disputes that "trademark.com" names are reserved to legitimate trademark holders, whereas "trademarksucks.com" names can be used legitimately for purposes of criticism and commentary consistent with the First Amendment.[256] Thus, the same may be said of political domain names—the "politicianname.com" version could be reserved to the politician, and other variations could be presumed to be available for otherwise lawful comment about the politician: that is, comment that is not defamatory or fraudulent.

Again, some of the California legislation relating to bad faith registrations and uses of domain names may prove to be a good legislative testing ground for these kinds of issues and might inform debate at the federal level—or at least lead to a more harmonized state-based approach to some of these issues.[257] Although a number of practical procedural problems arise with respect to legislation as opposed to revision of the UDRP, as discussed earlier,[258] value judgments about balancing rights to political speech in the electoral context might be best left to local judges interpreting local legislation, as opposed to arbitrators

---

[256] *See* Taubman Co. v. Webfeats, 319 F.3d 770, 778 (6th Cir. 2003) (holding that a "namesucks.com" domain was protected First Amendment commentary where there was no intent to sell); Lucent Techs., Inc. v. Lucentsucks.com, 95 F. Supp. 2d 528, 535–36 (E.D. Va. 2000) (suggesting "lucentsucks.com" could not be found to violate the trademark laws without infringing the registrant's free speech rights but deciding on other grounds); *see also* Lipton, *supra* note 23, at 1339–43 (discussing identifying and descriptive function of namesucks.com-type websites). But such a presumption is not uniformly accepted. *See* Chubb Sec. Austl. PTY Ltd. v. Tahmasebi, No. D2007-0769, ¶ 6(A) (WIPO Aug. 13, 2007), http://www.wipo.int/amc/en/domains/decisions/word/2007/d2007-0769.doc (stating there is a split in the decisions whether "trademarksucks.com" is permissible). *Compare* Societé Air Fr. v. Virtual Dates, Inc., No. D2005-0168, ¶ 6(A) (WIPO May 24, 2005), http://www.wipo.int/amc/en/domains/decisions/word/2005/d2005-0168.doc (finding "airfrancesucks.com" domain name was sufficiently confusing to consumers to order the name to be transferred to the relevant trademark holder, Air France), *with* Bridgestone Firestone, Inc. v. Myers, No. D2000-0190, ¶ 6 (WIPO July 6, 2000), http://www.wipo.int/amc/en/domains/decisions/word/2000/d2000-0190.doc ("The Panel sees no reason to require domain name registrants to utilize circumlocutions like <www.trademarksucks.com> to designate a website for criticism or consumer commentary."). For a detailed discussion of relevant case law in the commercial arena, see Margreth Barrett, *Domain Names, Trademarks, and the First Amendment: Searching for Meaningful Boundaries*, 39 CONN. L. REV. 973, 1012–15 (2007).

[257] *See* CAL. BUS. & PROF. CODE §§ 17525–17526 (West 1997 & Supp. 2007); CAL. ELEC. CODE §§ 18320–18323 (West 2003 & Supp. 2007).

[258] *See supra* notes 40–47 and accompanying text.

within a global system. Arbitrators may be well-versed in trademark law and domain name regulation generally, but may have little familiarity with local laws relating to free speech and the democratic process—and may have different cultural and political ideals in this context, depending on their respective locations and backgrounds.

B. *California's Political Cyberfraud Legislation*

Unsurprisingly, the PCAA appears to be a good legislative model expressly targeted at the kinds of conduct described in this Article as *political cyberfraud.* Even though the legislation is a good model, its provisions apparently apply more broadly than to simple protection of domain names from misleading and deceptive uses categorized here as cyberfraud.[259] Some of its provisions also cover conduct previously and more accurately categorized as cybersquatting.[260] Thus, there may be some difficulties and inconsistencies in applying the legislation in the political cyberfraud context. The legislation prohibits the three classes of conduct discussed previously: (a) attempts to deny a person access to a political website,[261] (b) attempts to deny a person the opportunity to register a domain name for a political website,[262] and (c) activities concerning a website that would cause a person to believe that the website actually represents the views of a proponent or opponent of a ballot measure.[263] Of these, classes (b) and (c) are probably the most relevant to the kind of conduct categorized here as political cyberfraud, although some such conduct may arguably fall within class (a).[264]

Class (a)—attempts to deny a person access to a political website—may be less relevant to political cyberfraud because if a person registers a domain name corresponding to a political actor's name to promulgate misleading or deceptive information about that person's political message,[265] she may or may not have actually "denied the person access to a political website." The access question might depend upon whether the person in question still had access to *any* relevant domain names to promulgate his own political message.[266] If the

---

[259] *See* CAL. ELEC. CODE § 18320(c)(1).

[260] *See id.*

[261] *Id.*

[262] *Id.*

[263] *Id.*

[264] *See* CAL. ELEC. CODE § 18320(c)(1).

[265] *See id.* Under the current PCAA, such a message would of course concern support of, or opposition to, a ballot measure. *See id.* § 18320(c)(3).

[266] *Id.* § 18320(c)(1).

domain name registrant had registered multiple domain names corresponding to the speaker's name and had cut off access to the most obvious iterations of the name, such as "name.com" and "name.org," this might be an example of cutting off access to a political website as contemplated in class (a).[267]

Activity falling under class (b)—attempts to deny a person the opportunity to register a domain name for a political website—contemplates situations where a person registers a domain name corresponding to a politician's name with a view to denying the politician the opportunity to register that domain name.[268] It is, of course, arguable that class (b) conduct may not be judicially interpreted this broadly under the PCAA if this provision were read as prohibiting attempts to deny a person the opportunity to register *any* domain name, as opposed to a particular domain name.[269] In other words, it is not clear on the face of the statute whether the prohibition applies only to situations where the domain name registrant has effectively cut off access to *any* relevant web presence via her registration of relevant domain names or has cut off access to *one specific* domain name.[270] The legislative phrase "to deny a person the opportunity to register a domain name for a political Web site" is ambiguous in this context.[271] Does the indefinite article refer to one or many domain names here? Again, one might need to consider precisely *which* iterations of the politician's name had been registered. The denial of "name.com" and "name.org" to the politician should perhaps raise more red flags than "namesucks.com" or than even the less pejorative, but also less intuitive, "nameinfo.com" or even "name.info."

Prohibiting conduct described by class (c) may be more promising for victims of the kind of political cyberfraud discussed in this Article.[272] This class refers to conduct that causes an Internet user to believe that a website has been posted by someone other than the person who posted it.[273] This class clearly contemplates prohibiting conduct where a person registers a domain name corresponding to a political speaker's name for the purposes of promulgating a misleading message about the person or her views.[274] Some of these situations may also be caught

---

[267] *See id.* It seems theoretically possible, however, that denying access to *any* of these could be denying access to "a" political website. *See id.*

[268] *See id.*

[269] CAL. ELEC. CODE § 18320(c)(1).

[270] *See id.*

[271] *See id.*

[272] *See id.*

[273] *See id.*

[274] CAL. ELEC. CODE § 18320(c)(1).

by defamation law, depending on the content of the website.[275] A statutory provision like the PCAA, however, could cast a broader net here and be cheaper and easier to litigate than defamation.[276] All that a victim of class (c) conduct would have to prove is that the way the website in question has been used suggests an affiliation that does not in fact exist.[277] This could be established by proving that the defendant had registered a domain name corresponding to the political speaker's name to provide information about the person or her purported message regardless of whether the messages were defamatory.[278] The "misleading" conduct conceived as political cyberfraud would simply be using the person's name in the domain name for an unauthorized, unofficial website about the person or her message.[279]

Taking this interpretation of class (c) conduct is somewhat akin to the developing trademark law principle that "trademark.com" names should be reserved to legitimate trademark holders on the basis that any other presumption would potentially mislead consumers or dilute the relevant trademark.[280] Taking this analogy further, it may be that registering a "namesucks.com" domain name would not fall afoul of this provision on the basis that adding an obviously pejorative term to the name in the domain space would not mislead Internet users to think that the site actually reflected the relevant person's views.[281]

In sum, legislative provisions like some of those found in the PCAA might be good models for providing politicians with some protection against political cyberfraud. Such provisions may prove to be an effective complement to defamation laws applied online to the extent that cyberfraud laws sufficiently protect politicians—and public expecta-

---

[275] *See* SILVERBERG, *supra* note 130, ¶ 6.01.

[276] *See* CAL. ELEC. CODE § 18320(c)(1).

[277] *See id.*

[278] *See id.*

[279] There may be some First Amendment concerns here as to whether, in this context, this provision, or any similar provision that may ever be debated at the federal level, would survive judicial scrutiny as a content-based restriction on First Amendment freedoms. At the date of writing, there is, as yet, no judicial interpretation on relevant issues, such as whether such a provision could be regarded as a content-based restriction on speech and, if so, whether it would survive strict scrutiny.

[280] *See* 15 U.S.C.A. § 1125(c)(1), (d) (West 1997 & Supp. 2007). Trademark "dilution" refers to unauthorized acts with respect to a famous mark "that tend to blur the distinctiveness of [the] mark or to tarnish the mark by using it in a disparaging or unsavory way." DEBORAH BOUCHOUX, INTELLECTUAL PROPERTY: THE LAW OF TRADEMARKS, COPYRIGHTS, PATENTS, AND TRADE SECRETS 103 (2000).

[281] *See Taubman*, 319 F.3d at 778 (holding that a "namesucks.com" domain was protected First Amendment commentary where there was no intent to sell, and finding no liability).

tions—against the kind of conduct contemplated here. Because *cyberfraud* is a somewhat more subjective term than *cybersquatting*, at least as contemplated in this Article, it may not matter if protection for politicians here is piecemeal and derives organically through the development of state legislation as interpreted by the courts. Ultimately, this might be the most effective way of developing appropriate legislative and judicial presumptions to facilitate speech during an election campaign in the most effective way possible—both to facilitate politicians disseminating their messages to voters as well as to facilitate general engagement with the political process by the public. Questions about where lines should be drawn between conduct that amounts to "cyberfraud" and legitimate comment about a politician should perhaps best be left to courts and state legislatures to develop over time.

Borrowing some presumptions from domain name disputes involving trademark rights may be useful here as described in the previous section.[282] An obvious example is the adoption of a presumption that "name.com" and perhaps "name.org" domains be reserved to relevant politicians, and other variations of those names such as "namesucks.com" or "namecommentary.com" should be made available for legitimate, if unauthorized, comments about politicians.[283]

C. *Laws Protecting Personal Reputation*

Some of the "personal reputation" laws discussed with respect to political cybersquatting may also have some application to political cyberfraud.[284] Defamation is an obvious contender here.[285] Also, the right of publicity may have some application, although this seems less likely because that right focuses on attempts to use a famous name or likeness to commercialize on the success of another, as opposed to commenting on another.[286] State legislation like the recently added provisions in the California's Business and Professions Code may have some application here, although it is more clearly directed to cybersquatting rather than cyberfraud.[287] As described previously relative to cybersquatting, subsection 17525(a) of the Business and Professions Code prohibits the bad faith registration, trafficking, or use of a domain name that is iden-

---

[282] *See* 15 U.S.C.A. § 1125(d)(1).

[283] *See id.*

[284] *See supra* notes 127–176 and accompanying text.

[285] *See* SILVERBERG, *supra* note 130, ¶ 6.01.

[286] *See* GILSON LALONDE ET AL., *supra* note 18, § 2.16[1].

[287] *See* CAL. BUS. & PROF. CODE § 17525(a) (West 1997 & Supp. 2007).

tical or confusingly similar to the personal name of another person.[288] This would certainly cover the registration or use of a domain name corresponding to a politician's name for "bad faith" purposes such as promulgating a misleading message about the politician.[289] Again, it will be the judiciary's task to establish the boundaries of "bad faith" in this context.[290] Looking at the legislative guidance on bad faith within the statute, three classes of conduct described in the legislation may be particularly relevant to political cyberfraud.[291] They are found in subsections 17526(e), (i), and (j) respectively.[292]

Subsection 17526(e) contemplates the following as a bad faith factor:

> The intent of a person . . . to divert consumers from the person's . . . online location to a site accessible under the domain name that could harm the goodwill represented by the person's . . . name either for commercial gain or with the intent to tarnish or disparage the person's . . . name by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site.[293]

As noted in the preceding discussion, this subsection is written in trademark-based language with its references to goodwill and likelihood of confusion.[294] As also acknowledged above, however, it is possible to draw some lessons for the political context from trademark presumptions developed in the domain space.[295] If the assumption is made that a website bearing a "name.com" or "name.org" domain is expected to resolve to an official website of the politician in question, it may well be regarded as bad faith conduct for someone other than the politician to create a website about the politician using such a name.[296]

Subsection 17526(e) is concerned with both profit and consumer confusion motives—which seem to connote both cybersquatting and

---

[288] *See id.*; *supra* notes 177–200 and accompanying text.
[289] *See* CAL. BUS. & PROF. CODE §§ 17525(a), 17626(j).
[290] *See id.* § 17525(a).
[291] *See id.* § 17526(e), (i), (j).
[292] *See id.*
[293] *Id.* § 17526(e).
[294] *See* 15 U.S.C. § 1125(a) (2000); CAL. BUS. & PROF. CODE § 17526(e).
[295] *See* 15 U.S.C.A. § 1125(d)(1) (West 1997 & Supp. 2007).
[296] *See id.*; CAL. BUS. & PROF. CODE §§ 17525(a), 17526(e).

cyberfraud.[297] Some cyberfraud will fall within the concept of confusing consumers about the endorsement of a particular website, regardless of whether the registrant had an intent to profit from selling the name.[298] By definition, whether the conduct will amount to cyberfraud will depend on the content of the website in conjunction with the use of a politician's name, unlike pure cybersquatting, which encompasses only the registration of the name and a bad faith attempt to profit from its sale, regardless of website content. Thus, subsection 17526(e) may cover either cybersquatting or cyberfraud or both at once, depending on the particular Internet presence at issue.[299] The use of a domain name corresponding letter-for-letter with a politician's name where the website promulgates misleading messages about the politician and also offers to sell the domain name to the highest bidder would clearly infringe section 17525 and amount to both cyberfraud and cybersquatting.[300] A simple attempt, however, to sell such a name without utilizing any web content about the politician could be prohibited under the legislation per se as cybersquatting but would not amount to cyberfraud.[301]

Subsection 17526(i) of the Code contemplates as an indicator of bad faith whether a domain name registrant "sought or obtained consent from the rightful owner to register, traffic in, or use the domain name."[302] If we presume that a politician is the "rightful owner" of a domain name corresponding to his personal name, this provision will certainly cover some cyberfraud.[303] Whether the conduct amounts to cyberfraud will always be context-specific and depend on the domain name actually registered and presumptions about the identity of the "rightful owner" of that name.[304] Though we may accept a presumption that Senator Hillary Clinton is the "rightful owner" of "hillaryclinton.com," is she also the rightful owner of other variations on her name like "hillaryclintonsucks.com," "hillarycriticism.com," or even "whyhillary.com," "voteforhillary.com," or "voteagainsthillary.com"? If we regard one single politician as the "rightful owner" of all variations of her

---

[297] *See* CAL. BUS. & PROF. CODE § 17526(e); *supra* notes 30–32 and accompanying text (defining cybersquatting); *supra* notes 235–238 and accompanying text (defining cyberfraud).

[298] *See* CAL. BUS. & PROF. CODE § 17526(e).

[299] *See id.*

[300] *See id.* § 17525(a).

[301] *See id.*

[302] *Id.* § 17526(i).

[303] *See* CAL. BUS. & PROF. CODE § 17526(i).

[304] *See id.*

name, this may well chill political speech overall.[305] By the same token, however, there should be some domain space reserved for legitimate political messages to be directly communicated by the relevant politician to the public.[306]

Finally, subsection 17526(j) of the Code contemplates as a bad faith factor the intent of a domain name registrant "to mislead, deceive, or defraud voters."[307] Although not so relevant to cybersquatting, this provision has particular relevance for cyberfraud because of its focus on the use of the name to interfere with the content of communications within the electoral process.[308] The provision must at least implicitly refer to the content of the relevant website and the relationship between web content and the domain name in question.[309]

Legislation such as California's Business and Professions Code may well have some role to play in developing the framework for political cyberfraud as well as potentially for political cybersquatting.[310] As with provisions of the PCAA, it may be worth treating California as a laboratory for testing how courts interpret all of this legislation with respect to both political cybersquatting and political cyberfraud.[311] Obviously, state legislation that has no, or few, analogs in other states can only provide a limited testing ground for the development of relevant principles.[312] It may be desirable for more states to experiment with such laws in the interests of developing clearer principles about the appropriate boundaries for domain name use in the electoral context, though this could also lead to disharmonization, particularly in the context of a federal election.[313]

---

[305] *Cf. Taubman*, 319 F.3d at 778.

[306] This is similar to the primary rationale for regulation in the broadcast area, where limitations are justified by the fact that the airwaves are limited. *See, e.g.*, Ellen P. Goodman, *Stealth Marketing and Editorial Integrity*, 85 TEX. L. REV. 83, 146 (2006) ("The first and most widely used rationale for broadcast regulation is that there is a finite number of frequencies that can be used productively and this number is far exceeded by the number of persons wishing to broadcast to the public.") (citations omitted). Similarly, there are likely a finite number of domain names corresponding to politicians' names that can be used productively by the politician.

[307] CAL. BUS. & PROF. CODE § 17526(j).

[308] *See id.*

[309] *See id.*

[310] *See supra* notes 177–200 and accompanying text.

[311] *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) (discussing role of state as legislative testing ground).

[312] *See id.*

[313] *See id.*

D. *Political Cyberfraud and the Anticybersquatting Regulations*

Like the California Business and Professions Code provisions, other regulations may also overlap in their application to both political cyberfraud and political cybersquatting.[314] The regulations aimed directly at cybersquatting, like the ACPA and the UDRP, may have applications in the cyberfraud area depending on the registrant's particular conduct.[315] Even though each of these regulatory measures is premised on domain name registration or use with a bad faith profit motive,[316] they may each apply to cases of cyberfraud where the profit motive overlaps with misleading or deceptive use of a domain name in a political website.[317] Of course, with one notable exception, neither of these regulatory measures is likely to apply in the absence of a trademark interest in the politician's name.[318] The exception is the "personal name" provision of the ACPA, which protects a person (including a politician) against a bad faith registration of a domain name corresponding to that person's name without that person's consent.[319]

Again, the theoretical basis of the consent requirement is not clear from the legislation. As the ACPA is a trademark protection statute, it would seem that the congressional power exercised here is the Commerce Clause power, used to create commercial property or property-like rights in domain names corresponding to personal names.[320] However, as noted in the previous Part, it would seem more theoretically satisfying, at least in the political context, to base any rights in a domain

---

[314] 15 U.S.C.A. §§ 1125(d)(1), 1129 (West 1998 & Supp. 2007); UDRP, *supra* note 14, ¶ 4(a).

[315] *See* 15 U.S.C.A. §§ 1125(d)(1), 1129; UDRP, *supra* note 14, ¶ 4(a).

[316] 15 U.S.C. § 1125(d)(1)(a)(i) (2000) ("[A] person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person . . . has a *bad faith intent to profit* from that mark . . . .") (emphasis added); *id.* § 1129(1)(A) ("Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, *without that person's consent, with the specific intent to profit* from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.") (emphasis added).

[317] See 15 U.S.C.A. §§ 1125(d), 1129; UDRP, *supra* note 14, ¶ 4(a).

[318] See 15 U.S.C.A. §§ 1125(d), 1129; UDRP, *supra* note 14, ¶ 4(a).

[319] 15 U.S.C. § 1129(1)(A) ("Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.").

[320] *See* Planned Parenthood Fed'n of Am., Inc. v. Bucci, 42 U.S.P.Q.2d (BNA) 1430, 1435–39 (S.D.N.Y. 1997) (noting congressional jurisdictional predicate in Lanham Act is based on events occurring "in commerce").

name corresponding to a politician's name on notions of democratic government rather than commercial property.[321] The personal name provisions of the ACPA were not primarily directed at politics, although some domain name arbitrators have suggested that these provisions are the most effective way for a politician who does not have a trademark interest in her personal name to protect it against unauthorized incursions in the domain space.[322]

The main problem with the personal name provisions in the ACPA is that they will not apply to any kind of cyberfraud unless there is a corresponding cybersquatting motive.[323] In other words, if there is no bad faith *actual intent to sell* the domain name in question, the personal name protections in the ACPA will not apply.[324] Thus, if a registrant utilized a domain name corresponding to a politician's name to make comments about the politician, no action would lie unless the complainant could prove the registrant actually at some point intended to sell the domain name to the politician or to someone else.[325] Thus, the ACPA provisions will be limited to cases involving cybersquatting, even if they do also involve cyberfraud.[326] As such, they do not add much to a discussion of pure cyberfraud that does not involve such a bad faith profit-seeking motive.[327]

---

[321] *See* STEPHEN J. BREYER, ACTIVE LIBERTY 39 (2005); *supra* note 255 and accompanying text.

[322] Friends of Kathleen Kennedy Townsend v. Birt, No. D2002-0451, ¶ 6 (WIPO July 31, 2002), http://www.wipo.int/amc/en/domains/decisions/word/2002/d2002-0451.doc ("This does not mean that Complainant is without remedy. The ACPA contains express provisions protecting the rights in personal names."). This is because the ACPA does not require a politician or anyone else to establish a common law or registered trademark interest in her name to seek a remedy. *See* 15 U.S.C. § 1129.

[323] 15 U.S.C. § 1129(1)(A).

[324] *Id.* ("Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, *with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party,* shall be liable in a civil action by such person.") (emphasis added).

[325] *Id.*

[326] The same is technically true of the more trademark-focused provisions of the ACPA found in § 1125(d). That section requires a bad faith profit motive, although not necessarily a sale motive. *See* 15 U.S.C.A. § 1125(d)(1)(A)(i) (West 1998 & Supp. 2007) (setting out the requirement of a "bad faith intent to profit" from a trademark in a trademark-based cybersquatting action, as distinct from an action to protect personal names under § 1129(1)(A)).

[327] Dogan & Lemley, *supra* note 48, at 1203 (noting in the celebrity personal name context that even though the ACPA "captures pure cases of celebrity cybersquatting . . . , cases in which the registration of a domain name is used to mislead visitors will have to be addressed in other ways").

The UDRP may be a little different here.[328] Although, like the ACPA, it is premised on notions of bad faith cybersquatting, it is slightly broader in its terms of coverage.[329] To establish a claim under the UDRP, a complainant needs to establish that the registrant: (a) has a domain name that is identical or confusingly similar to a trademark in which the complainant has rights,[330] (b) has no rights or legitimate interests in the name,[331] and (c) has registered and used the domain name in bad faith.[332] Unlike an ACPA action, neither the actual intent to sell the name[333] or make some other form of profit from the name in bad faith[334] is necessary for a successful UDRP arbitration.[335] Instead, the main problem of addressing political cyberfraud under the UDRP will be for a politician to establish trademark rights in his personal name.[336] If he can establish such rights, then it may be possible for him to bring a cyberfraud claim under the UDRP if he can prove that the registrant has no legitimate interest in the name and has used it in bad faith.[337]

The next problem in applying the UDRP to political cyberfraud would be in establishing the boundaries of "legitimate" use and "bad faith" in this context.[338] The UDRP itself gives little guidance here.[339] Although UDRP arbitrators in the past have recognized free speech as a "legitimate interest,"[340] this has occurred in the case of deciding the

---

[328] *See* UDRP, *supra* note 14, ¶ 4(a)(iii) (requiring bad faith in domain name registration and use).

[329] *Compare* 15 U.S.C. § 1129 (requiring intent to sell domain for profit), *with* UDRP, *supra* note 14, ¶ 4(a)(iii), (b) (requiring registration and use "in bad faith" and setting out nonexclusive bad faith factors).

[330] UDRP, *supra* note 14, ¶ 4(a)(i).

[331] *Id.* ¶ 4(a)(ii).

[332] *Id.* ¶ 4(a)(iii).

[333] *See* 15 U.S.C. § 1129(1)(A) (requiring intent to profit from the domain name with respect to personal names to be actionable).

[334] *See* 15 U.S.C.A. § 1125(d)(1)(A)(i) (West 1998 & Supp. 2007) (requiring bad faith with respect to trademark-based domain name protections).

[335] *See* UDRP, *supra* note 14, ¶ 4(a) (requiring bad faith but not necessarily a profit).

[336] *See supra* notes 78–88 and accompanying text (discussing problems that may be faced by politicians in trying to establish trademark interests in personal names used purely for political purposes); *see also* Townsend v. Birt, No. D2002-0030, ¶ 6 (WIPO Apr. 11, 2002), http://www.wipo.int/amc/en/domains/decisions/word/2002/d2002-0451.doc (failing to protect Townsend's name under the UDRP).

[337] *See Clinton*, No. FA0502000414641 (finding Hillary Clinton could establish common law trademark rights in the "Hillary Clinton" mark); UDRP, *supra* note 14, ¶ 4(a).

[338] *See* UDRP, *supra* note 14, ¶ 4(a).

[339] *See id.*

[340] *See Bridgestone Firestone*, No. D2000-0190, ¶ 6. The UDRP "legitimate use" factors do not contemplate free speech *per se* and are limited to the various legitimate commercial

boundaries of protecting commercial trademark interests, not political disputes.[341] Some have also presumed that free open discourse will be protected in this context provided that the registrant has not usurped the ".com" version of the name that rightfully belongs to the trademark holder.[342] It is obviously arguable that if free speech is protected as a legitimate interest under the UDRP in the commercial context, it should definitely be so protected in the political context. But the assumption in the commercial context is that the speech itself on the relevant website is "legitimate": that is, the speech is a legitimate critique or commentary of the relevant trademark holder.[343] It may be more difficult in the political context to establish whether particular speech is legitimate or, rather, amounts to "cyberfraud" because of the higher protections placed on protecting political speech over commercial speech in many jurisdictions.[344] In other words, the boundaries of legitimate political speech under the UDRP may be broader than the boundaries of legitimate commercial speech, suggesting political domain names might be more difficult to preserve for the politician's message. Establishing these boundaries may thus be a very difficult task to place on the shoulders of UDRP arbitrators who are predominantly trained in commercial trademark law and not

---

uses set out in clause 4(c) of the UDRP. This list is not exclusive so arbitrators have had some leeway to expand on it. *See id.* (discussing question of whether fair use and free speech are defenses to a claim for transfer of a domain name under the UDRP and noting "[t]he Internet is above all a framework for global communication, and the right to free speech should be one of the foundations of Internet law").

[341] *See id.*

[342] *Id.* ("In this case, the Respondent's principal purpose in using the domain name appears not to be for commercial gain, but rather to exercise his First Amendment right to criticize the Complainants. The use of the <trademark.net> domain name appears to be for the communicative purpose of identifying the companies, which are the subject of his complaints. He is not misleadingly diverting users to his website, as he has not utilized the <.com > domain and has posted adequate disclaimers as to the source of the website. It does not appear that his actions are intended to tarnish, or have tarnished, the Complainants' marks.").

[343] *Id.*

[344] *See, e.g.*, N.Y. Magazine v. Metro. Transit Auth., 987 F. Supp. 254, 260 (S.D.N.Y. 1997) ("Speech is generally protected unless it falls in a category that removes it from the scope of First Amendment protection .... In order to determine the protection to be afforded to the speech in issue, it is necessary to decide whether it is entitled to full First Amendment protection or to the more limited protection accorded to what is known as 'commercial speech.' Once upon a time commercial speech was 'deemed wholly outside the purview of the First Amendment.' ... Since 1976, however, the Supreme Court has consistently held that such speech is protected although it 'is entitled to a lesser degree of protection than other forms of constitutionally guaranteed expression.'" (quoting Gordon and Breach Sci. Publishers S.A. v. Am. Inst. of Physics, 859 F. Supp. 1521, 1536 (S.D.N.Y. 1994)).

constitutional law in any given jurisdiction. UDRP arbitrators on the international level may not be the best arbiters of where those boundaries should lie in the political context.[345]

As with the "legitimate interests" test under the UDRP,[346] the "bad faith" use test[347] is drafted in terms of commercial trademark uses, for example, misleading consumers as to affiliation or source of a particular good or service.[348] The two "bad faith factors" that may be relevant to political cyberfraud are the following: first, evidence that the domain name has been acquired primarily for the purpose of selling it to a rightful trademark holder or to a competitor of that trademark holder; and, second, evidence that the name has been acquired to prevent the trademark holder from reflecting its mark in a corresponding domain name.[349] Although both of these factors are premised on the complainant holding trademark rights in the relevant name, a politician might be able to use them where she can establish that she holds such trademark rights.[350]

E. *Regulating Cyberfraud vs. Regulating Cybersquatting*

Probably the most confusing aspects of attempts to regulate political cyberfraud relate to understanding the relationship between political cyberfraud and political cybersquatting, and the reasons for distinguishing between the two. It is easy to take a "scattergun" approach to regulation of both classes of conduct.[351] In fact, this describes the current regulatory situation.[352] It is a pastiche of laws that generally at-

---

[345] Of course, a counterargument to this is that the UDRP is only intended to protect commercial trademark interests. *See* UDRP, *supra* note 14, ¶ 4(a)(i). In the context of protecting trademarks corresponding to politicians' names, maybe UDRP arbitrators are really only being asked to resolve the dispute to the extent it is commercial, not where it is purely political. Nevertheless, isolating the commercial component could be confusing in practice if the politician in question is really concerned with defamation or other noncommercial reputational damage. It may be better to label such situations "pure cyberfraud" situations and litigate them under relevant laws such as defamation or anticyberfraud laws, discussed above.

[346] *Id.* ¶ 4(c).

[347] *Id.* ¶ 4(b).

[348] *Id.* ¶ 4(b)(iv).

[349] *Id.* ¶ 4(b)(i), (ii).

[350] *See Clinton*, No. FA0502000414641 (finding that Senator Clinton had established common law rights in the "Hillary Clinton" mark to grant UDRP standing).

[351] *See* 15 U.S.C.A. §§ 1125(d), 1129 (West 1998 & Supp. 2007); CAL. BUS. & PROF. CODE §§ 17525–17527 (West 1997 & Supp. 2007); CAL. ELEC. CODE. §§ 18320–18323 (West 2003 & Supp. 2007); UDRP, *supra* note 14, ¶ 4(a).

[352] *See* 15 U.S.C.A. §§ 1125(d), 1129; CAL. BUS. & PROF. CODE §§ 17525–17527; CAL. ELEC. CODE. §§ 18320–18323; UDRP, *supra* note 14, ¶ 4(a).

tempts to regulate all bad faith conduct relating to domain names, political or otherwise.[353] The problem is that these regulations have developed quickly in recent years with insufficient scrutiny of precisely what conduct should be proscribed, particularly in a political context. Identifying the exact classes of conduct in question, as this Article attempts to do, will help greatly in tailoring appropriate regulations and remedies that do the least damage to political discourse.

Current regulatory measures overlap in a seemingly vague way with respect to political cyberfraud and political cybersquatting, as demonstrated in the above discussion, despite the fact that the two classes of conduct raise quite different concerns and call for different kinds of remedies.[354] Although both classes of conduct may overlap in some situations, overlap is not invariable.[355] Political cybersquatting potentially wastes political communications channels, whereas political cyberfraud involves fraudulent and misleading uses of a political domain name.[356] Political cybersquatting can thus be regulated fairly simply and mechanically—either a domain name is being used in a wasteful manner or it is not. Implementing a simple arbitration procedure should be able to determine this wastefulness question.[357] On the other hand, political cyberfraud raises substantive questions of the relationship between speech content and a domain name that are better regulated by those who are experts in identifying and balancing legitimate political speech against illegitimate communication. Where the two classes of conduct coincide in a given case, a complainant should be entitled to decide between the relevant remedial mechanisms and should be able to avail herself of both if necessary.

The problem is that current laws do not differentiate effectively between the two classes of conduct and, to the extent that the terms *political cybersquatting* and *political cyberfraud* are used at all, they tend to

---

[353] *See* CAL. SENATE JUDICIARY COMM., COMMITTEE ANALYSIS OF A.B. 277, 2003–04 Reg. Sess., at 4–5 (July 8, 2003), http://info.sen.ca.gov/pub/03-04/bill/asm/ab_0251-0300/ab_277_cfa_20030709_163232_sen_comm.html (discussing instances of bad faith conduct but without discussion of overlapping cyberfraud and cybersquatting concerns as defined in this Article).

[354] *See id.*; 15 U.S.C.A. §§ 1125(d), 1129; CAL. BUS. & PROF. CODE §§ 17525–17527; CAL. ELEC. CODE. §§ 18320–18323; UDRP, *supra* note 14, ¶ 4(a).

[355] *See supra* notes 299–301 and accompanying text (discussing conduct which could be cybersquatting but not cyberfraud).

[356] *See supra* notes 165–166 and accompanying text (discussing greater expense of speech where cybersquatting interferes); *supra* notes 235–238 and accompanying text (defining cyberfraud).

[357] *See supra* notes 124–126 and accompanying text (discussing potential expansion of UDRP to mitigate political cybersquatting).

be used somewhat interchangeably.[358] This will likely cause confusion and problems interpreting relevant regulations as political campaigns increasingly rely on the Internet and on the domain name system in particular.[359] Now may also be the time to start unraveling and understanding some of the policies underlying the regulation before the confusion becomes entrenched in the domain name system.[360] Such confusion over the underlying theory behind the existing rules has already become entrenched in the system in the purely commercial context, involving the interpretation of the ACPA and the UDRP in trademark-based domain name disputes.[361] The problem is largely because of a failure to identify and categorize appropriately the competing classes of interests that need to be protected and balanced in the domain name system with respect to trademarks.[362] Some regulatory forethought and planning could avoid similar problems in the political context.

III. Politicians' Names vs. Trademarks

A. *"Hillary.com": A Case Study*

The preceding discussion argued in favor of identifying two specific categories of bad faith conduct involving domain names corresponding to politicians' names—political cybersquatting and political cyberfraud—and with developing appropriate legal responses to each. One additional situation, however, that can arise regarding political domain names, albeit rarely, involves a coincidental cross-over between the commercial trademark system and the political system. It concerns the situation where a commercial trademark interest happens to correspond to a politician's name, and both parties desire use of a corre-

---

[358] *See supra* notes 95–126, 259–283 and accompanying text (discussing California's political cyberfraud legislation, which covers aspects of both cyberfraud and cybersquatting); *supra* notes 314–327 and accompanying text (discussing anticybersquatting regulations of the ACPA, which can cover aspects of cyberfraud as it coincides with cybersquatting in practice).

[359] PEW Internet & Am. Life Project, *supra* note 1, at 1–10.

[360] *See* Lipton, *supra* note 10, at 1431. *See generally* Lipton, *supra* note 23.

[361] *See* Lipton, *supra* note 10, at 1369–81. *See generally* Lipton, *supra* note 23.

[362] *See* Lipton, *supra* note 10, at 1364 ("The time has come to develop some new approaches to domain name disputes that can take account of interests in domain names outside the bad-faith cybersquatting context. This Article suggests a new classification scheme for different kinds of domain name disputes. The new scheme can serve as the basis for the development of new approaches to Internet domain name dispute resolution .... [This Article] identifies the kinds of competing social values that will likely need to be taken into account in future development of a more comprehensive approach to domain name dispute resolution.").

sponding domain name. An obvious example could arise in the situation of the "hillary.com" domain name. Many people would likely think such a name would relate to Senator Hillary Clinton. Upon typing the domain name into a web browser, however, one would find that the name resolves to a webpage administered by a company, Hillary Software, Inc., which appears to be a legitimate company with a corresponding trademark or business name.[363]

Although this may be confusing in one sense for Internet users looking for Senator Clinton's website, it is obviously—or at least apparently—not an attempt to hijack her name as a domain name to extort money from her for transfer of the name.[364] It is also not an attempt to provide any information about the senator under a relevant domain name.[365] It is, of course, possible that if Senator Clinton wanted that domain name for herself she might make an offer for the name to Hillary Software, but the company would be under no legal obligation to accept her offer, having seemingly legitimately registered a domain name corresponding to its business name and trademark and having used the name purely for its own commercial purposes in the software industry.[366]

Presuming that the registrants of "hillary.com" have registered and used the name in good faith for their own business purposes, they will not have contravened any existing laws based on protecting trademark rights in corresponding Internet domain names.[367] This will be the case whether or not Senator Clinton is regarded as having a trademarked or trademarkable personal name.[368] In any event, trademarked or not, and registered as a mark or not, Senator Clinton could not likely establish trademark infringement by Hillary Software, because of the lack of consumer confusion.[369] It is unlikely that web users looking for infor-

---

[363] *See* Hillary Software, Inc., http://www.hillary.com (last visited Oct. 28, 2007).

[364] *See id.*

[365] *Id.*

[366] *See* 15 U.S.C.A. § 1125(d) (West 1998 & Supp. 2007); CAL. BUS & PROF. CODE § 17525 (West 1997 & Supp. 2007).

[367] *See* 15 U.S.C.A. § 1125(d).

[368] In fact, Senator Clinton has been regarded in at least one UDRP arbitration as having a common law trademark interest in her name. Clinton v. Dinoia a/k/a SZK.com, No. FA0502000414641 (NAF Mar. 18, 2005), http://www.arb-forum.com/domains/decisions/414641.htm. The arbitrator ordered a transfer of the "hillaryclinton.com" name to Senator Clinton largely on this basis. *Id.* However, that arbitration was undefended and there was no evidence that the registrant of the domain name was using it for any legitimate purpose, unlike potentially the registrant of "hillary.com." *See id.*

[369] *See* 15 U.S.C. § 1125(a)(1)(A) (2000). This is perhaps similar to the results that occur in cases involving competing legitimate interests in trademarks where only one associ-

mation about Senator Clinton and her policies would think that the Hillary Software website had anything to do with her.[370] It is possible she might argue that Hillary Software is creating what has come to be called "initial interest confusion"; that is, where consumers are initially confused on reaching a website and are then diverted from pursuing their original search object.[371] But again, it is unlikely that Internet users seeking information about Senator Clinton would find information about a software firm to be a sufficient diversion to deter them from searching for Senator Clinton's actual website.

Senator Clinton would additionally be unlikely to establish an infringement of the ACPA provisions protecting personal names because such an action would require that the corresponding domain name be registered with "the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party."[372] Assuming that Hillary Software did not register its "hillary.com" name for this purpose, it is unlikely to run afoul of this provision.[373]

Senator Clinton would also be unlikely to succeed against the registrant of "hillary.com" in a UDRP arbitration because the registrant could likely demonstrate its legitimate use of the domain name under the UDRP criteria.[374] In particular, the registrant appears to be using the domain name in connection with a bona fide offering of computer software services.[375] For similar reasons, it is unlikely that Hillary Software has run afoul of any existing state laws, notably the California laws relating to unfair business practices and political cyberfraud.[376] If there

---

ated domain name is available. *See* Hasbro, Inc. v. Clue Computing, Inc., 66 F. Supp. 2d 117, 126 (D. Mass. 1999) (holding that Hasbro failed to show consumer confusion for trademark infringement purposes with respect to the use of the "clue.com" domain name by Clue Computing). In *Hasbro Inc. v. Clue Computing, Inc.*, despite Hasbro's registration of the "Clue" trademark for its popular board game of the same name, it was unable to establish that the use of the "clue.com" domain name by Clue Computing was confusing Hasbro's consumers as to the source or origin of relevant goods or services. *See id.*

[370] *See* 15 U.S.C. § 1125(a) (prohibiting trademark infringement based on likelihood of confusion as to source).

[371] Even though Internet users would not necessarily be confused once they arrived at the site for which they were not actually searching, some courts consider the likelihood of confusion requirement met by "initial interest confusion." *See supra* note 112.

[372] *See* 15 U.S.C. § 1129(1)(A).

[373] *See id.*

[374] UDRP, *supra* note 14, ¶ 4(c).

[375] *Id.* ¶ 4(c)(i).

[376] *See* CAL. BUS. & PROF. CODE § 17525(a) (West 1997 & Supp. 2007); CAL. ELEC. CODE § 18320 (West 2003 & Supp. 2007). This assumes that these laws could even apply to Internet conduct affecting a New York senator, and that the election code provisions re-

is no bad faith for the purposes of the unfair business laws such an action would not likely succeed.[377] Furthermore, without any willful intent to deceive electors, cyberfraud legislation as currently conceived would not apply.[378] Moreover, if there is no content about Senator Clinton on the relevant website, as indeed there is not in the case of "hillary.com," proceedings under defamation or celebrity tort laws by Senator Clinton would also likely be inapplicable.[379]

It is possible that Senator Clinton could succeed in a trademark dilution action,[380] presuming she has a famous trademark interest here.[381] Such an action is premised on the notion of tarnishing or blurring of a mark.[382] In other words, dilution decreases the ability of a mark to operate as a mark and identify relevant goods and services.[383] The problem with dilution law is that it is premised on the notion that the underlying mark be famous and be used in connection with the sale of goods or services.[384] It is not clear that Senator Clinton's personal name would qualify on either count, although it is possible.[385] In any event, it is unclear that the software company's use of the name

---

garding ballot measures could apply at all in this situation. *See* CAL. BUS. & PROF. CODE § 17525(a); CAL. ELEC. CODE § 18320(c)(1)–(3).

[377] *See* CAL. BUS. & PROF. CODE § 17525(a).

[378] *Cf.* CAL. ELEC. CODE §§ 18320–18323.

[379] That they are unlikely to be helpful is because these actions are premised on comments about the plaintiff in the case of defamation, or attempts to usurp the commercial value of a celebrity's persona in the case of the celebrity tort. *See supra* notes 284–286 and accompanying text. In the defamation case, Clinton would also probably have to surmount the high actual malice standard applicable to public figures. *See* N.Y. Times v. Sullivan, 376 U.S. 254, 279–80 (1964) (establishing actual malice standard for public figure defamation plaintiffs); *see also* Monitor Patriot Co. v. Roy, 401 U.S. 265, 271–72 (1971) (applying *New York Times* standard to political candidates).

[380] 15 U.S.C.A. § 1125(c)(1) (West 1998 & Supp. 2007) (prohibiting trademark dilution).

[381] Although personal names are not trademarkable without first attaining secondary meaning, *see* GILSON LALONDE ET AL., *supra* note 18, § 2.03[4][d], a UDRP panel did find the senator to have a common law trademark interest in "Hillary Clinton." *Clinton*, No. FA0502000414641. It is not clear whether this finding would extend to protection of "Hillary" alone as a mark *per se*. Further, the UDRP panel's comments would not be binding on a domestic court or even a later arbitration panel. There may also be questions as to whether the mark is sufficiently "famous" to support a trademark dilution action. *See* 15 U.S.C.A. § 1125(c)(1).

[382] 15 U.S.C.A. § 1125(c)(1).

[383] *Id.* § 1125(c) (defining dilution).

[384] *See id.*

[385] *See id.*

would, in fact, be regarded as either "blurring" or "tarnishing" any sufficiently famous trademark held by Senator Clinton.[386]

Is the answer for politicians, particularly those considering a presidential run, to register all relevant permutations of their personal names as domain names as quickly as possible[387] and hope that no legitimate trademark holders have beaten them to it? At least a politician who registers the name first might have more of a chance if a corresponding trademark holder later complains about the registration, particularly if the politician, like Senator Clinton, could establish some form of common law trademark rights in her own name,[388] or at least the absence of bad faith in the registration and use of the name.

This "get in first" solution would remedy potential cyberfraud and cybersquatting concerns as well. It is obviously not very realistic, however. For one thing, politicians—and prospective politicians—do not always know if and when they are likely to enter a political campaign and it seems unnecessarily distracting to expect them to vigilantly register every possible permutation of their personal name in a domain space at all times for avoidance of later problems—or at least the most obvious permutations of their name.[389] For another thing, politicians do not always want to advertise their prospective political

---

[386] *See* Dogan & Lemley, *supra* note 48, at 1197–1200 (noting, in the context of celebrity names, that dilution actions are not often likely to succeed because it will be difficult for the plaintiff to establish blurring or tarnishment even if the relevant name is sufficiently famous to support a dilution action). "Blurring" is generally regarded as "the whittling away of an established trademark's selling power through its unauthorized use upon dissimilar products." *See* BOUCHOUX, *supra* note 280, at 104 (stating that tarnishment occurs when a mark is linked to products of inferior quality compared with those the mark is meant to identify, or when the mark is portrayed in an unwholesome or embarrassing context).

[387] *See* Friess, *supra* note 9.

[388] When Senator Clinton brought an arbitration proceeding under the UDRP against the original registrant of "hillaryclinton.com," the arbitrator found that Senator Clinton did have common law trademark rights in the "Hillary Clinton" mark that corresponded to the "hillaryclinton.com" domain name. *Clinton*, No. FA0502000414641. The arbitrator ordered a transfer of the name to Senator Clinton largely on this basis. *Id.* However, that arbitration was undefended and there was no evidence that the registrant of the domain name was using it for any legitimate purpose, unlike potentially the registrant of "hillary.com". *See id.*

[389] For example, Senator Clinton may be much more interested in ensuring that an unauthorized party does not register "hillary.com" and "hillaryclinton.com" as opposed to the perhaps less intuitive names like "hillary2008.com," which at least at one point was apparently registered to a Mr. Brett Maverick of Canberra, Australia, and "hrc2008.com," which is currently registered to a company called "mrp inc." that may well be a cybersquatter. *See* Friess, *supra* note 9 (discussing domain registration of hillary2008.com); Whois.net, WHOIS Information for hrc2008.com, http://www.whois.net/whois_new.cgi?d=hrc2008.com&tld=com (last visited Oct. 15, 2007).

ambitions with such registrations, but registration alone is likely to become public because registration information is generally publicly available on "whois" searches.[390]

Politicians may also attempt to register their personal names federally as tradèmarks,[391] on the assumption that their name as a mark might ultimately develop sufficient secondary meaning to support the registration.[392] This may give them some additional ammunition under the trademark infringement and dilution provisions of the Lanham Act against various unauthorized activities involving registration and use of domain names corresponding to their personal names.[393] Not all politicians' names in a purely political context will, however, be able to support an ongoing federal registration.[394] In fact, as discussed earlier, not all politicians' names will even be able to attract common law trademark status.[395]

---

[390] *See* Whois.net, http://www.whois.net/ (last visited Oct. 15, 2007) (providing searchable database of domain name registration by domain name).

[391] 15 U.S.C. § 1052(c) does place restrictions on registration of personal names, but would not technically prevent an application for registration of a personal name as a mark *by the person whose name it is*, as opposed to an attempt to register by someone else without that person's consent. *See* 15 U.S.C. § 1052(c) (2000). The main problem would be establishing sufficient secondary meaning to support the ongoing registration. *See* GILSON LALONDE ET AL., *supra* note 18, § 2.03[4][d] ("Just as with descriptive terms, a trademark or trade name that consists of a personal name (first name, surname, or both) is entitled to legal protection only if it attains secondary meaning."); *id.* § 2.03[1] ("A descriptive term is not subject to legal protection unless it has attained secondary meaning, that is, the public has come to regard it as the trademark of one seller. At that point, the term becomes entitled to legal protection in order to prevent confusion, deception and mistake.").

[392] In general, a personal name will only be entitled to legal protection as a trademark if it has acquired a secondary meaning associating it with particular goods or services. GILSON LALONDE ET AL., *supra* note 18, § 2.03[4][d]. The problem for many politicians is that their names do not function in this way. If used purely in politics, the name may not be sufficiently associated with commercial goods or services to attract trademark protection—either on the federal register or at common law.

[393] Certainly trademark infringement and dilution actions are premised on the complainant holding a mark corresponding to a relevant name, *see* 15 U.S.C. §§ 1114(1), 1125(a)(1) (2000), and the UDRP requires the existence of a trademark right before it will grant relief. *See* UDRP, *supra* note 14, ¶ 4(a). Additionally, the basic anticybersquatting provisions of the ACPA require a trademark interest to grant relief, *see* 15 U.S.C.A. § 1125(d)(1)(A) (West 1998 & Supp. 2007), although the additional "personal name" provisions do not require a trademark corresponding to a personal name in order to grant relief. 15 U.S.C. § 1129 (2000).

[394] *See supra* note 392.

[395] *See* Friends of Kathleen Kennedy Townsend v. Birt, No. D2002-0451, ¶ 6 (WIPO July 31, 2002), http://www.wipo.int/amc/en/domains/decisions/word/2002/d2002-0451.doc (UDRP panel suggesting that the politician Kathleen Kennedy Townsend would not have a common law trademark in her personal name used for purely political purposes).

B. *Politicians vs. Legitimate Trademark Owners*

There are other more workable solutions to conflicts between politicians and legitimate trademark holders with interests in the same domain name, particularly in the electoral context. One solution would be a temporary compulsory licensing system under which a politician could exercise rights in the name in the lead-up to an election, and the name could thereafter revert to the legitimate trademark holder.[396] This system could be administered through domestic legislation or through the private administration and dispute resolution proceedings of the domain name system. The latter might be easier and would only involve adopting a simple dispute resolution scheme, like the UDRP, to be implemented in a similar way through contract with domain name registrants.[397] The difference would be that a private scheme would require domain name arbitrators to make determinations as to who has a better right to a given domain name in the lead-up to an election.[398] It would also have to give such arbitrators the power to order a temporary licensing measure in favor of a politician. The trademark holder would receive a set royalty fee for the use of the name during the license period. This would compensate for losing the commercial use of the name and may deter politicians from arbitrating for names they do not really need. Nevertheless, these kinds of arrangements may cause problems for the trademark owner wanting to use the relevant site. A temporary license in favor of the politician may be problematic as disrupting the business of the commercial trademark holder. Also, the politician may want to maintain the site after the election.[399] At this point, should he be forced to buy the name from the trademark holder for a reasonable market price?[400]

---

[396] Lipton, *supra* note 10, at 1433–35 (advocating for a compulsory licensing scheme or domain name sharing scheme for political domain names).

[397] *See generally* UDRP, *supra* note 14.

[398] *See generally id.*

[399] For example, Senator John Kerry has maintained his "johnkerry.com" website (last visited Oct. 15, 2007) subsequent to the 2004 presidential election to communicate with the electorate and, presumably, with the thought that he may again run for president in the future.

[400] Lipton, *supra* note 10, at 1434 ("There might . . . be situations in which a political candidate wants to retain a domain name past a temporary licensing period . . . . In such cases, provisions might be made for the compulsory license to continue until one or both parties to the license loses interest in, or use for, the domain name in question. Alternatively, if a particularly long-term license appears to be developing due to ongoing circumstances in which the name is potentially useful to both parties, provision might be built into the relevant scheme for a final sale of the name, assuming a fair market price could be reached between the parties.").

In any event, even without a licensing system in place, these kinds of disputes would likely only arise in rare cases. Some politicians may not care about all commercial registrations of domain names corresponding to their personal names provided that relevant websites do not include any misleading comments about their campaigns, and provided that other intuitive domain names are available for their campaigns. Again, Senator Clinton may be a good example here. She may not care that Hillary Software is using the "hillary.com" name for legitimate commercial purposes, so long as they do not allow that name to be used for purposes that might impugn her campaign messages in a misleading way, and so long as she herself can use another equally intuitive domain name such as "hillaryclinton.com."[401]

Another potential solution for the rare case of a conflict between a legitimate trademark holder and a politician over a domain name could be a "domain name sharing" order.[402] This arrangement could be achieved in exactly the same procedural manner as the domain name licensing arrangement suggested above, but the administrative order could require the politician and the trademark holder to share the relevant domain name rather than requiring the trademark holder to license it to the politician. Under this arrangement, the domain name in question would resolve to a page simply containing hyperlinks to the relevant websites, in this case, one hyperlink to the commercial trademark holder's website and the other to the politician's website.[403] This kind of arrangement is possible with current Internet technologies and may create a more fair and efficient balance between commercial speech and political speech in these rare cases. It may also deter registration of political domain names under "sham" business names that look on their face like legitimate uses but are really set up in the hope

---

[401] She does in fact hold this name at the time of writing as a result of a UDRP ruling in 2005. *See Clinton*, No. FA0502000414641.

[402] *See* Lipton, *supra* note 10, at 1411–13; *see also* Jacqueline Lipton, *A Winning Solution for Youtube and Utube? Corresponding Trademarks and Domain Name Sharing*, HARV. J.L. & TECH. (forthcoming 2008) (suggesting an expanded UDRP procedure to encompass domain name sharing orders in cases where competing trademark holders can assert similar interests in the same domain name).

[403] This has occasionally been done already in the private commercial context. For example, the trademark "playtex" and the domain name "playtex.com" are used by two separate companies in two separate product markets. They share the domain name "playtex.com" which is then hyperlinked to the respective home pages of each individual company. Playtex Products, Inc. & HBI Branded Apparel Enterprises, LLC (Playtex Apparel), http://www.playtex.com (last visited Oct. 15, 2007) (stating that the Playtex companies are two separate entities with a shared name, and linking to "PlaytexProducts.com" and "PlaytexBras.com").

of extorting money from a politician for transfer of the name: in other words, another form of political cybersquatting.

It may also have some application in the rare case of a conflict between a politician and another person with a similar personal name, for example, if a politician like Chris Dodd or Joe Biden shares a name with a private citizen. In the absence of a trademark interest in either name, it may be that sharing the name is a viable option. In the absence of a sharing—or perhaps licensing—arrangement in this scenario, presumably the "first come, first served" rule under the domain name registration system would govern. The Lanham Act provisions, including the ACPA, are limited to bad faith conduct with respect to domain names relating to trademarks[404] and personal names,[405] as is the UDRP.[406] If the private citizen had registered the name first and was not making bad faith use of the name, presumably she would be safe from an ACPA or UDRP challenge.[407] This is where a sharing or licensing scheme may be particularly useful. Alternatively, a rule could be developed for these cases at the local or international level that the use of the name within the political process "outranks" the use of the name for a private individual in order to maximize the communicative potential of the Internet in an electoral context. Clearly, this would have to be the result of policy discussions amongst Internet governing bodies and perhaps also at the international level.

Conclusions and Future Directions

The use of domain names and associated web content will increase in the political context in coming years. The Internet is an unprecedented communication medium in terms of being an incredibly low-cost method of reaching a tremendously large audience.[408] As more and more people are connected to the Internet, and as politicians and their campaign managers become more and more conversant with its potential, the problems politicians face due to bad faith conduct involving

---

[404] 15 U.S.C.A. § 1125(d)(1)(A)(i) (West 1998 & Supp. 2007).

[405] *Id.* § 1129(1)(A).

[406] UDRP, *supra* note 14, ¶ 4(a), 4(c)(ii). The UDRP's protection is limited to trademarked personal names unlike the ACPA, which will protect personal names more generally. *See* 15 U.S.C.A. § 1129(1)(A); UDRP, *supra* note 14, ¶ 4(a).

[407] *See* 15 U.S.C.A. § 1125(d)(1)(B)(i) (citing bad faith factors for cybersquatting); UDRP, *supra* note 14, ¶ 4(b) (listing nonexclusive bad faith considerations).

[408] *See* Internet Communications, 71 Fed. Reg. 18,589, 18,589–91 (Apr. 12, 2006) (distinguishing Internet from print and other media as lower cost and nearly unlimited).

Internet domain names will also magnify.[409] That is why it is imperative to start thinking about how the Internet in general, and the domain name system in particular, should be regulated in the political context as soon as possible. Although some scholarly attention has been paid to questions of domain name regulation in the context of commercial trademark disputes,[410] little thought has been given to the protection of domain names used in politics. The particular issues raised in politics merit independent debate and perhaps specifically targeted solutions.

Some people may argue that the use of domain names in politics is simply a detail in a larger picture of regulating the Internet more broadly. There are several answers to this view. Although it may be true that much about the Internet in general, and the domain name system in particular, needs to be examined from a regulatory perspective at this point in time, there is something very special about the political process in a representative democracy that may well require separate attention. The electoral process is fundamental to the U.S. system of government, and the ability to disseminate and receive important information about politics and politicians in an electoral context is key to the functioning of that system. The need for electors and politicians to have every chance to participate fully in the political process, both as recipients and disseminators of relevant information, is of prime importance here. Thus, the operation of the domain name system as a directory for such information must be facilitated by the legal system to the maximum extent possible.

The use of domain names as guides to relevant information about politicians, particularly in an electoral context, also points to an answer to a second possible criticism of the approach to political domain name regulation advocated in this Article. Some would argue that focusing at all on the regulation of domain names misses the point of what needs to be regulated on the Internet. Commentators have noted in the past that search engines are now taking on prime importance as ways to navigate the Internet and that, as a result, the use of easy-to-remember domain names is less important than in the past.[411] Although this shift

---

[409] See PEW INTERNET & AM. LIFE PROJECT, *supra* note 1, at iv.

[410] *See generally* Barrett, *supra* note 256; Lipton, *supra* note10; Lipton, *supra* note 23.

[411] Goldman, *supra* note 112, at 548 ("Some searchers, frustrated with the DNS's low relevancy or adverse consequences, like typosquatting, porn-napping, and mousetrapping, may have become trained to start *every* search at a search engine instead of entering domain names into the address bar. For some searchers, search engines have supplanted DNS's core search function of delivering known websites. In turn, top search engine placements have eclipsed domain names as the premier Internet locations.").

may well be true as a general proposition, this argument only considers one perspective—the ability of sophisticated search engines to find information as a result of a particular search query. In other words, search engines clearly assist with information location, regardless of domain name, but they do not necessarily help with the *identificatory* function played by many Internet domain names.[412]

As with titles of books, songs, and movies, Internet domain names serve at least two functions. One is to describe the content of the underlying work or, in the case of a domain name, the underlying web content.[413] The other is to serve almost as a label to *identify* the work.[414] This enables people to refer to the relevant work (or, in the domain name case, the webpage) by name when talking to others about it.[415] It is clearly easier for me to refer a friend to, say, "factcheck.org" by referring to its domain name than by referring to its general content or the search steps I took to locate it using a particular search engine.[416] Even when search engines are used to locate a relevant webpage, some research suggests that web users will often remember domain names in any event and simply type them into a search engine rather than a web browser.[417] This is further evidence that the actual domain name retains its importance even when users increasingly rely on search engines to locate web content.[418] Additionally, even in the search engine context, many search engines will prioritize webpages with relevant domain names, depending on the search algorithms used.[419] Thus, domain names will retain their importance, despite the rise of increasingly sophisticated search engine technologies.

---

[412] *See* Lipton, *supra* note 23, at 1339–43; *cf.* GILSON LALONDE ET AL., *supra* note 18, § 2.03[1] (discussing identifying and distinguishing function of trademarks).

[413] Lipton, *supra* note 23, 1339–43.

[414] *Id.*

[415] *Id.*

[416] Although, ironically, it was not so easy for Vice President Cheney to refer to this website in the vice presidential debate leading up to the 2004 presidential election. Harry Chen Thinks Aloud, http://harry.hchen1.com/2004/10/06/89 (Oct. 6, 2004). He mistakenly referred to "factcheck.com" when he intended to refer to "factcheck.org," and people who looked up "factcheck.com" were redirected to George Soros' anti-President Bush website. *See id.*; *see also* Nick Anderson, *.com or .org? Cheney Suffers Slip of the Suffix*, L.A. TIMES, Oct. 7, 2004, at A19; Mark Memmot, *Cheney Error Sends Net Users Off Track: Viewers Directed to an Anti-Bush Site Instead of Online Fact-Checking Project*, USA TODAY, Oct. 7, 2004, at 11A.

[417] Goldman, *supra* note 112, at 548.

[418] *See id.*

[419] *See* GILSON LALONDE ET AL., *supra* note 18, § 7A.08 (discussing use of search terms of trademarks in domain names and in website coding to produce search engine results).

Thus, the regulation of domain names within the global information society is likely to maintain an important place in future debates about Internet governance generally. As described throughout this Article, the electoral process raises specific issues relating to domain names that are not clearly dealt with by the current regulatory system, and are not really at the forefront of current debate, although they should be. This Article has been concerned with three distinct classes of conduct, all of which have raised some concerns in the political process. To date, however, these classes of conduct have not yet been clearly categorized or examined with respect to the specific issues they raise for the political process and the domain name system.

Ultimately, resolving some of these issues may be an incidental part of resolving some other domain name questions relating to the protection of personal names in the domain space more generally.[420] The ACPA provisions relating to the protection of personal names against bad faith cybersquatting are a good example of a law concerned with a broader question that may incidentally protect some politicians' names against certain classes of bad faith conduct online.[421] Nevertheless, the development of regulations protecting personal names generally has not been a priority of the international legal community, although there are some domestic examples of laws in this area.[422] Domain name conflicts involving politicians' names and campaigns require more speedy attention than they have received to date. Their resolution is certainly more important than resolving issues concerning personal names that do not affect the political process in any significant way. This is because of the fundamental importance of the political process and the exponentially increasing use of the Internet in the political context.[423]

There are undoubtedly problems relating to domain names in politics that have not been canvassed in any detail within this Article. Intentional "misspellings" of politicians' names within domain names, for example, have been only incidentally addressed here. This is because they largely raise the same issues as accurate spellings of politicians' names in the domain space and, as such, should be similarly separated out into the relevant categories of conduct. A deliberate misspelling of Senator

---

[420] For example, one option for the protection of personal names generally would be to extend the UDRP's reach to cover personal names and not just trademarks. *See* UDRP, *supra* note 14, ¶ 4(a); *supra* notes 124–126 and accompanying text.

[421] *See* 15 U.S.C.A. §§ 1125(d), 1129 (West 1998 & Supp. 2007).

[422] *See, e.g., id.*; CAL. BUS. & PROF. CODE § 17525(a) (West 1997 & Supp. 2007); CAL. ELEC. CODE §§ 18320–18323 (West 2003 & Supp. 2007).

[423] *See* PEW INTERNET & AM. LIFE PROJECT, *supra* note 1, at iv.

Obama's name for the purposes of cybersquatting, for example, should be treated in the same way as an accurate spelling of his name. Thus, a person who registered, say, "www.barakobama.com" in the hope of extorting money from Senator Obama for transfer of the name to him, should be subject to any rules developed to protect against a cybersquatter who had registered "www.barackobama.com" with a similar purpose.[424] By the same token, anyone who registered the misspelling with the intention of making false and defamatory comments about the senator might be subject both to defamation law in terms of the content and to a cyberfraud regulation of the kind described in this Article in terms of the association of the false content with the domain name.

The main aim of this Article has been to attempt to focus some of the future debate on Internet governance on the issue of protecting political names in the domain space. The key point is that the current system does not adequately protect politicians' names in the domain space against various forms of bad faith conduct. Current regulatory measures—focused largely on protecting commercial trademark interests in cyberspace—do not effectively facilitate purely political discourse through appropriate and effective use of the domain name system. In order to address the problems raised by the current system, it is first necessary to categorize the problems, as this Article has attempted to do, and then to debate potential solutions to them. Hopefully the above discussion has provided some useful first steps in this direction, and the debate over Internet governance can in the future better accommodate the needs of the modern political process.

---

[424] *See* 15 U.S.C. § 1129(1) (2000) (prohibiting use of personal name cybersquatting, including a name confusingly similar to a living person's name). At the date of writing, "barackobama.com" seems to be registered legitimately to Senator Obama's campaign, but "barakobama.com" may be registered to a supporter intending to protect Senator Obama from either or both of the types of conduct discussed in this Article. *See* Whois.net, WHOIS Information for barakobama.com, http://whois.net/whois_new.cgi?d=barakobama&tld=com (last visited Sept. 20, 2007) (stating "barakobama.com" belonged to "Registered to Protect from Squatters"). Of course, "Registered to Protect from Squatters" could be a squatter itself. *See id.*