September 2014

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

Jacqueline D. Lipton
Case Western Reserve University School of Law, jdl14@case.edu

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? Although, for example, Senator Hillary Clinton now owns 'hillaryclinton.com', the more generic 'hillary.com' is registered to a software firm, Hillary Software, Inc. What about 'hillary2008.com'? It is registered to someone outside the Clinton campaign and is not currently in active use. 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 is focused 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) politicial '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.

TABLE OF CONTENTS

* Professor, Co-Director, 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 Professor Mark Janis for comments on an earlier iteration of this article. All mistakes or omissions are my own.

INTRODUCTION

Who owns 'hillary.com'? Or 'obama.com'? Or 'guiliani.com'? How important might some of these names be in the lead-up to the next presidential election? If past history is anything to go by, 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. The 'kerryedwards.com' 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.[1] Internet domain names are becoming increasingly important in political campaigns to identify political websites both for fundraising purposes, and to disseminate information about relevant policy issues. An Internet presence is now invaluable for a politician. 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. In some respects this potentially levels the playing field for politicians and political commentators alike regardless of their fund raising abilities.

[1] See *Nobody Wants Kerryedwards.Com*, August 3, 2004 (last viewed on March 14, 2007, and available at http://www.networkworld.com/weblogs/layer8/005859.html) (discussing attempt by Mr Kerry Edwards to auction the domain name kerryedwards.com to the highest bidder during the course of the 2004 presidential election).

However, an Internet presence with an easy-to-guess and easy-to-recognize domain name can cause problems for politicians. 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,[2] and not on protecting political interests.[3] There are significant gaps in the law when it comes to the use of domain names in politics. 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 legitimately used in the political process. Conversely, there are no clear rules prohibiting socially wasteful or blatantly misleading use of political domain names.

The current domain name regulation system is focused on preventing trademark-based cybersquatting. 'Cybersquatting' in this context has been described as speculatively purchasing a domain name with the intention of selling it for a profit[4] – usually with respect to a well-known name corresponding with a trademark.[5] 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 it will only protect trademarked, and therefore *trademarkable*, political domain names, and the second is that it will only protect those names against bad faith cybersquatting. These are serious limitations. Many policitican's names will not be trademarkable[6] and much of the abusive conduct that arises in an electoral context involves misleading *content* on a political website rather than an attempt to sell a particular political domain name for a profit.

This article makes several important contributions to the debate on facilitating effective political speech in cyberspace. The first is to create a novel categorization scheme for the various types of domain name registrations that may cause problems for politicians. The development of this categorization scheme is essential in the political context. In fact, the lack of a categorization system in the trademark context has caused

---

2 Jacqueline Lipton, *Beyond Cybersquatting: Taking Domain Names Past Trademark Policy*, 40 WAKE FOREST L R 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.")

3 *id*, 1425-1431 (discussion of the gaps in current regulations in the political context).

4 Ira Nathenson, *Showdown at the Domain Name Corral: Property Rights and Personal Jurisdiction over Squatters, Poachers and Other Parasites,* 55 U PITT L REV 911, 925-926 (1997).

5 "Cybersquatting" is currently defined in the Wikipedia as: "is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else. The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price." (last viewed on March 14, 2007 and available at http://en.wikipedia.org/wiki/Cybersquatter).

6 Generally, personal names are not registrable as trademarks: 15 U.S.C. § 1052 (c). See also GILSON ON TRADEMARK PROTECTION AND PRACTICE, ¶ 2.03[d].

many problems of development and interpretation of the domain name regulationsystem in recent years.[7] 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. 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. 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. Part III deals with the more unusual situation involving competitions between trademark holders and politicians with similar names – for example, Hillary Software, Inc.[8] and Senator Hillary Clinton if they both wanted the 'hillary.com' domain name. Part IV provides conclusions and suggests options for future developments in political domain name regulation.

II. POLITICAL CYBERSQUATTING

A. POLITICIANS' NAMES AND THE ANTI-CYBERSQUATTING CONSUMER PROTECTION ACT

Political cybersquatting may be defined as the political analog to traditional cybersquatting. It would include registration and use of a domain name corresponding with a politician's name with the intent to sell the domain name for a profit to the politician or to a third party. While the conduct is similar – and similarly motivated – in both the trademark and the political contexts, different legal and theoretical issues arise. Traditional cybersquatting involves people registering often multiple domain names corresponding with registered trademarks with the intent to profit from selling the names to the relevant trademark holders or a third party.[9] This conduct was originally prohibited under trademark infringement[10] and dilution[11] law. Later, additional

---

[7] See, for example, discussion in Margreth Barrett, *Domain Names, Trademarks, and the First Amendment: Searching for Meaningful Boundaries*, 39 CONNECTICUT L R 973 (2007); Jacqueline Lipton, *Commerce vs Commentary: Gripe Sites, Parody and the First Amendment in Cyberspace*, forthcoming, WASHINGTON UNIVERSITY L R, 2007; Jacqueline Lipton, *Beyond Cybersquatting: Taking Domain Names Past Trademark Policy*, 40 WAKE FOREST L R 1361 (2005).

[8] The current holder of the 'hillary.com' domain name.

[9] "Cybersquatting" is currently defined in the Wikipedia as: "is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else. The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price." (last viewed on March 14, 2007 and available at http://en.wikipedia.org/wiki/Cybersquatter); see also 15 U.S.C. § 1125(d).

[10] 15 U.S.C. §§ 1114(1)(a), 1125(a)(1) – statutory prohibitions against trademark infringement at the federal level for registered and common law marks respectively, premised on creation of consumer

regulatory measures were taken to proscribe this conduct. In the United States, the Anti-Cybersquatting Consumer Protection Act ('ACPA') was inserted into the Lanham Act[12] in 1999 to combat this conduct. This legislation prohibits the practice of cybersquatting and sets out a number of 'bad faith factors'[13] that courts can use in determining whether or not particular conduct falls within the notion of a bad faith intent to profit from registration of a relevant domain name.

At roughly the same time, the Internet Corporation for Assigned Names and Numbers ('ICANN')[14] adopted the Uniform Domain Name Dispute Resolution Policy ('UDRP')[15] to achieve similar ends. The UDRP has been extremely popular in practice because it is implemented under private contract between domain name registrants and domain name registrars[16] and hence has a more global reach than domestic legislation. 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.[17] The arbitrations are fast,[18] inexpensive,[19] and largely online procedures[20] that can result

---

confusion as to source of relevant goods or services. See also *Planned Parenthood Federation of America v Bucci*, 42 U.S.P.Q. 2d 1430 (S.D.N.Y., 11997) (for an example of the use of traditional trademark infringement law to prohibit unauthorized bad faith registration and use of a domain name corresponding with someone else's registered trademark).

11 15 U.S.C. §§ 1125(c), 1127 (federal statutory prohibitions on trademark dilution – the lessening of the capacity of a famous mark to identify or distinguish goods or services regardless of consumer confusion). See also *Panavision Int'l v Toeppen*, 141 F 3d 1316 (9th Cir, 1998) (an example of a successful trademark dilution action against cybersquatting).

12 15 U.S.C. Chapter 22.

13 15 U.S.C. § 1125(d)(1)(B)(i).

14 The body that regulates the domain name system: see www.icann.org for further information.

15 The full text of the UDRP is available at: http://www.icann.org/udrp/udrp-policy-24oct99.htm (last viewed on March 14, 2007).

16 UDRP, clause 2 ("By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else's rights.")

17 UDRP, clause 4(a) ("You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, 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.")

18 A domain name arbitration will generally take less time than judicial proceedings, typically taking around two months for a decision to be issued. See *InterNic FAQs on the Uniform Domain Name Dispute Resolution Policy (UDRP)*, last viewed on March 14, 2007 and available at: http://www.internic.net/faqs/udrp.html.

in transfer of a domain name to a rightful owner[21] if the complainant can establish to the arbitration panel's satisfaction that the registration or use of the domain name was in bad faith[22] and the registrant had no legitimate purpose for registering the name.[23]

Political cybersquatting, however, is not always covered by these laws, particularly if the politician's name in question is not considered to be trademarked or trademarkable.[24] This will certainly be true of traditional trademark infringement[25] and dilution actions,[26] and also general trademark-based anti-cybersquatting actions under the ACPA.[27] While some additional anticybersquatting laws do deal specifically with the protection of individual's names against bad faith cybersquatting even in the absence of a trademark interest in the name, [28] they may be limited in application. The obvious example of an anti-cybersquatting law that protects non-trademarked personal names

---

[19] The range of fees for an arbitration will be around $1,000-$2,000 for a single arbitrator panel and a little more for a larger panel. See *InterNic FAQs on the Uniform Domain Name Dispute Resolution Policy (UDRP)*, last viewed on March 14, 2007 and available at: http://www.internic.net/faqs/udrp.html.

[20] Rules for Uniform Domain Name Dispute Resolution Policy, last viewed on March 14, 2007 and available at: http://www.icann.org/udrp/udrp-rules-24oct99.htm: Rule 3(b) (complaint to be submitted in hard copy and electronic format); Rule 5(b) (response to be submitted in hard copy and electronic format); Rule 13 (no in-person hearings); Rule 16(b) (Panel decisions to be posted on panel web site).

[21] UDRP, clause 4(i) ("The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.").

[22] UDRP, clause 4(b).

[23] UDRP, clause 4(c).

[24] Generally, personal names are not registrable as trademarks: 15 U.S.C. § 1052 (c). See also GILSON ON TRADEMARK PROTECTION AND PRACTICE, ¶ 2.03[d].

[25] 15 U.S.C. §§ 1114(1)(a), 1125(a)(1) (federal statutory prohibitions against trademark infringement for common law and registered marks respectively, premised on creation of consumer confusion as to source of relevant goods or services.)

[26] 15 U.S.C. §§ 1125(c), 1127 (federal statutory prohibitions on trademark dilution prohibiting the lessening of a mark's capacity to distinguish particular goods or services regardless of consumer confusion).

[27] 15 U.S.C. § 1125(d) (prohibition of cybersquatting based on registration of a domain name similar to a trademark).

[28] 15 U.S.C. § 1129 (this section protects personal names against cybersquatting and is not limited to trademark interests in personal names).

against cybersquatting is § 1129 of the Lanham Act,[29] introduced in 1999 as part of the ACPA:[30]

> 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.[31]

This will cover some political cybersquatting, although there will also be exceptions. In the 'kerryedwards.com' scenario,[32] for example, it might technically have been possible for the registrant, Mr Kerry Edwards, to mount several defenses to an ACPA challenge. He might have argued that the domain name in question did not correspond to the name of another living person on the basis that 'Kerry Edwards' was not the name of either Senator Kerry or Senator Edwards, but rather an amalgam of both of their names. 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 equally be protected by §1129.

With respect to the first argument, the defense might fail on the basis that § 1129 also protects complainants against bad faith registrations of domain names that are 'substantially and confusingly similar' to their own personal names. 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 names are those on the presidential ticket would be considered a registration of a name 'substantially and confusingly similar' to the Senators' respective personal names. The second potential defense argument may be more problematic, but 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 the name.

---

[29] 15 U.S.C. § 1129.

[30] This provision is to be distinguished from 15 U.S.C. § 1125(d) which is also part of ACPA but 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.

[31] 15 U.S.C. § 1129(1)(A).

[32] See *Kerry Edwards is Real and Sells Kerryedwards.Com*, July 19, 2004, last viewed on March 14, 2007 and available at: http://www.editorsweblog.org/news/2004/07/kerry_edwards_is_real_and_sells_kerryedw.php ("KerryEdwards.com is owned by a 34-year-old man named Kerry Edwards, a part-time bail bondsman in Indianapolis. He registered KerryEdwards.com two years ago as a personal site for family and friends.")

There were two additional 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.[33] 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* the domain name[34] with the intent to profit from its sale as required by § 1129.[35] 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 with the two names on the presidential ticket. This is unlikely to happen in many future cases. However, it is possible that a private individual might have a personal name corresponding with an individual politician's name in a future case and this could raise many of the difficulties that could have arisen had 'kerryedwards.com' been disputed 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, not to mention Barack Obama. 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 situations where a private individual's name may correspond with a relevant domain name, there are a few other practical problems with the ACPA provisions protecting personal names from bad faith registrations. One is that it does not have a global reach, although at least a federal statute is better in terms of legal harmonization than a pastiche of often-piecemeal state laws.[36] The other problem with § 1129 of the Lanham Act is arguably 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. 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.[37] This is not surprising, but, as recent UDRP arbitrations

---

33 *id.*

34 As opposed to having *used* it.

35 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). 15 U.S.C. § 1125(d) would not have applied here because the 'Kerry Edwards' name was not trademarked, nor was it likely trademarkable in the electoral context: Generally, personal names are not registrable as trademarks: 15 U.S.C. § 1052 (c). See also GILSON ON TRADEMARK PROTECTION AND PRACTICE, ¶ 2.03[d].

36 See discussion of some relevant Californian state laws in Parts ___, *infra*.

37 For example, *Roberts v Boyd*, Case No. D2000-0210 (WIPO Arb. and Mediation Ctr., Admin. Panel Decision, May 29, 2000) (involving the Julia Roberts name) (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html); *Springsteen v Burgar*, Case No D2000-1532 (WIPO Arb. and Medication Ctr., Admin. Panel Decision, Jan. 5, 2001) (involving Bruce Springsteen's name) (last viewed on march 14, 2007 and available at

have shown, the UDRP is not as easily geared to combat cybersquatting involving *any* personal names, let alone political personal names, as § 1129 of the Lanham Act.

B. POLITICIANS' NAMES AND THE UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY

As already noted, the UDRP contains certain procedural advantages for a complainant concerned with an act of bad faith cybersquatting. Its main limitation in the context of political cybersquatting is that it does not specifically protect personal names against bad faith registrations and uses. 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.[38] Even some politicians have succeeded here.[39] The problem has been that, in the absence of a specific protection for personal names under the UDRP, complainants must successfully assert a trademark interest in their personal names.[40] This can sometimes be done quite easily:

---

http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1532.html); *Rita Rudner v. Internetco Corp.*, (WIPO Case No. D2000-0581, August 3, 2000) (involving Rita Rudner's personal name) (last viewed on March 14, 2007 and available at: http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0581.html); *Helen Folsade Adu, known as Sade v. Quantum Computer Services Inc.*, (WIPO Case No. D2000-0794, Sep. 26, 2000) (involving Sade's stage name) (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0794.html); *Friends of Kathleen Kennedy Townsend v Birt* (WIPO Case No D2002-0451) (involving Kathleen Kennedy Townsend's name) (last viewed at March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0451.html); *Ciccone v Parisi* (WIPO Case No D2000-0847)(involving the singer Madonna's stage name) (last viewed on March 14, 1007 and available at: http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0847.html); *Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com* (National Arbitration Forum Claim No. FA0502000414641, March 18, 2005) (involving the domain name 'hillaryclinton.com') (last viewed on March 14, 2007 and available at http://www.arb-forum.com/domains/decisions/414641.htm).

[38] For example, *Roberts v Boyd*, Case No. D2000-0210 (WIPO Arb. and Mediation Ctr., Admin. Panel Decision, May 29, 2000) (involving the Julia Roberts name) (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html); *Ciccone v Parisi* (WIPO Case No D2000-0847)(involving the singer Madonna's stage name) (last viewed on March 14, 1007 and available at: http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0847.html).

[39] *Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com* (National Arbitration Forum Claim No. FA0502000414641, March 18, 2005) (involving the domain name 'hillaryclinton.com') (last viewed on March 14, 2007 and available at: http://www.arb-forum.com/domains/decisions/414641.htm).

[40] UDRP, clause 4(a)(i) (complainant must establish trademark interests corresponding with relevant domain name as one of the bases for her complaint). This was certainly played out in domain name disputes corresponding with the personal names of Julia Roberts, Madonna and Hillary Clinton. UDRP arbitrators established that all of these people had trademark interests in their personal names to support their UDRP complaints. See *Roberts v Boyd*, Case No. D2000-0210 (WIPO Arb. and Mediation Ctr., Admin. Panel Decision, May 29, 2000) (involving the Julia Roberts name) (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html); *Ciccone v Parisi* (WIPO Case No D2000-0847)(involving the singer Madonna's stage name) (last viewed on March 14, 1007 and available at: http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0847.html);

for example, some celebrities do hold registered trademarks in their names if they use them as commercial trademarks.[41] In other cases, UDRP arbitrators have been prepared to accept common law trademark rights in a famous celebrity's[42] or politician's name.[43]

However, in the case of even famous personal names of celebrities and politicians, UDRP arbitrators do not always accept a trademark interest on the part of the complainant. When Bruce Springsteen and his management initiated a UDRP arbitration for transfer of the 'springsteen.com' name from a registrant utilizing it for an unauthorized fan website,[44] the majority arbitration panelists were not convinced that even a celebrity as popular as Springsteen necessarily had a common law trademark right in his personal name.[45] In the political context, Kathleen Kennedy Townsend failed to

---

Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com (National Arbitration Forum Claim No. FA0502000414641, March 18, 2005) (involving the domain name 'hillaryclinton.com').

[41] For example, the singer Madonna has registered Madonna as a trademark. See *Ciccone v Parisi* (WIPO Case No D2000-0847)(involving the singer Madonna's stage name) (last viewed on March 14, 1007 and available at: http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0847.html), ¶ 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.")

[42] For example in the Julia Roberts case: *Roberts v Boyd*, Case No. D2000-0210 (WIPO Arb. and Mediation Ctr., Admin. Panel Decision, May 29, 2000) (involving the Julia Roberts name) (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0210.html), ¶ 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.")

[43] For example in the case of the 'hillaryclinton.com' domain name: *Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com* (National Arbitration Forum Claim No. FA0502000414641, March 18, 2005) (last viewed on March 14, 2007 and available at http://www.arb-forum.com/domains/decisions/414641.htm) ("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.")

[44] *Springsteen v Burgar*, Case No D2000-1532 (WIPO Arb. and Medication Ctr., Admin. Panel Decision, Jan. 5, 2001) (involving Bruce Springsteen's name) (last viewed on march 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1532.html).

[45] *id*. ¶ 6 ("It is common ground that there is no registered trade mark in the name "Bruce Springsteen". In most jurisdictions where trade marks are filed it would be impossible to obtain a registration of a name of that nature. Accordingly, Mr Springsteen must rely on common law rights to satisfy this element of the three part test. It appears to be an established principle from cases such as Jeanette Winterson, Julia Roberts, and Sade that in the case of very well known celebrities, their names can acquire a distinctive secondary meaning giving rise to rights equating to unregistered trade marks, notwithstanding the non-registerability of the name itself. It should be noted that no evidence has been given of the name "Bruce Springsteen" having acquired a 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. In the view of this Panel, it is by no means clear from

convince UDRP arbitrators[46] that she had a trademark interest in her personal name in the context of a gubernatorial election in Maryland.[47] Interestingly, the panel suggested that supporters of Townsend may have been able to assert a trademark interest in her name,[48] and that Townsend herself may have successfully brought an action under § 1129 of the Lanham Act.[49]

It has been suggested that the UDRP be revised to incorporate provisions protecting personal names from bad faith registration and use.[50] However, to date, no revisions have been made and the World Intellectual Property Organization ('WIPO') has suggested further inquiry into the need for such revisions.[51] It should be borne in mind that the UDRP is a global arbitration process. 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,[52] such as in § 1129 of the Lanham Act. On the global scale, there are more names and presumably more people, even potentially famous people, with similar or the same names. Additionally, different legal systems may well take differing

---

the UDRP that it was intended to protect proper names of this nature. As it is possible to decide the case on other grounds, however, the Panel will proceed on the assumption that the name Bruce Springsteen is protected under the policy; it then follows that the domain name at issue is identical to that name.")

46 *Friends of Kathleen Kennedy Townsend v Birt* (WIPO Case No D2002-0451) (involving Kathleen Kennedy Townsend's name) (last viewed at March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0451.html).

47 *id*, ¶6 ("The Panel finds 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.**")**

48 *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.")

49 *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.

50 WIPO, Second WIPO Internet Domain Name Process: The Recognition of Rights and the Use of Names in the Internet Domain Name System, Sept 3, 2001 (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/processes/process2/report/html/report.html#5), ¶¶179-205.

51 *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.")

52 See discussion of this issue in WIPO, Second WIPO Internet Domain Name Process: The Recognition of Rights and the Use of Names in the Internet Domain Name System, Sept 3, 2001 (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/processes/process2/report/html/report.html#5), ¶¶179-205.

attitudes to the protection of personal names in the domain space, whether they be political names, celebrity names, or private individual's names.[53]

C. APPLICATION OF CYBERFRAUD LEGISLATION TO POLITICAL CYBERSQUATTING

There are some other possible legal avenues for politicians concerned about political cybersquatting. California's Political Cyberfraud Abatement Act ('PCAA'),[54] for example, prohibits engaging in acts of 'political cyberfraud' which 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…".[55] Some aspects of this may cover political cybersquatting, even though it is notionally directed at conduct described as *cyberfraud*.[56]

Political cybersquatting would not likely be covered by the third statutory prohibition on 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. This is because the point of cybersquatting is to sell the name for a profit rather than to make misleading use of the site. 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 politician while at the same time trying to sell the domain name. However, the 'misleading information' part of such conduct is categorized throughout this article as 'political cyberfraud' rather than 'political cybersquatting'. This is 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.

It is possible that political cybersquatting would be included in the first two prohibitions in the Californian PCAA. It may count as conduct intended to deny a person access to a political website or to deny a person the opportunity to register a domain name for a political website. The PCAA further defines political cybersquatting activities as including, but not being limited to, the following conduct:

---

53 *id.*

54 Cal. Elec. Code, §§ 18320-23 (Deering Supp. 2005).

55 *Id*., § 18320(c)(1).

56 "Political cyberfraud" is defined in § 18320(c)(1) of the California Elections Code rather broadly as: "a knowing and willful act concerning a political Web site 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, and would cause a reasonable person, after reading the Web site, to believe the site actually represents the views of the proponent or opponent of a ballot measure …".

> (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 ….[57]
> (C) Registering a domain name that is similar to another domain name for a political Web site.[58]
> (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.[59]

These are all examples of conduct that might deny a politician access to a relevant domain name, although they may not all technically amount to political cybersquatting. A person who engages in political cybersquatting might not necessarily be regarded as having 'intentionally diverted or redirected access to a political web site to another website by the use of a similar domain name'. In situations where the politician in question has not yet registered a relevant domain name, it would be difficult to argue that access was being 'diverted' or 'redirected' from the politician's website to another website. If the politician never had a website to begin with, this provision may have no application, although it may well apply to a situation where the politician does have a website, but has not registered all possible permutations of the relevant domain name.

Senator Barack Obama, for example, has registered 'barackobama.com', but at the time of writing does not appear to have registered 'barack.com' or 'obama.com'. If someone else registered either of these names, as indeed currently appears to be the case with 'barack.com', Senator Obama may be able to bring a successful complaint under the PCAA[60] on the basis that the name diverts web users from his own website. Presumably, he would have to prove this to be the case in practice. It is not clear what would be necessary in this context: for example, would he simply have to 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?[61]

---

57 *id*, § 18320(c)(1)(A).

58 *id*, § 18320(c)(1)(C).

59 *id*, § 18320(c)(1)(D).

60 *id*, § 18320(c)(1)(A).

61 This would be similar to the 'initial interest confusion' doctrine that has arisen in the commercial trademark context with respect to 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. 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, for example, *Brookfield Communications Inc v West Coast Entertainment Corp*, 174 F 3d 1036, 1054-1064 (9th Cir 19999); Eric Goldman, *Deregulating Relevancy in Internet Trademark Law*, 54 EMORY LAW JOURNAL 507, 559 ('[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."; *Panavision Int'l v Toeppen*, 141 F 3d 1316 (9th Cir., 1998) (consumers would not actually have been confused as to source by defendant's website, but may have been distracted from finding the plaintiff's actual web presence).

Similar comments may be made about sub-section (C) *supra*. 'Registering a domain name that is similar to another domain name for a political website' may not include situations where the politician in question has not yet registered a domain name corresponding with her personal name. However, where the politician in question already does have a web presence, this sub-provision may be more useful than sub-section (A) because it does not require the complainant to establish an intent to divert or redirect access to the website. It only requires registration of a name that is similar to an existing political domain name.

Sub-section (D) looks to be much more directed at the kind of conduct described in this article as 'political cybersquatting' than the other provisions. 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 its use, or both.' This does not appear to require the politician in question to have already registered any domain name. It would cover a situation where a politician 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 politician.

However, the drafting of this provision may still be somewhat problematic in the situations described here as 'political cybersquatting'. For one thing, the provision does not cover situations where the registrant of the domain name is prepared to sell the domain name to the politician for a profit. It only appears to cover situations where the registrant is attempting to prevent a politician from using the name. Thus, it would 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 its use by Senator Obama. It does not seem to contemplate a situation where the registrant specifically attempts to sell the name to Senator Obama for a profit.

There are also jurisdictional problems with the application of the PCAA. Currently, California is the only state with such legislation. It is not clear whether this legislation would apply in situations where neither the politician in question nor the domain name registrant is located in California. It is possible that the ability of web users to access the website in California would be a sufficient connection with California for the Californian law to apply.[62] Additionally, it is possible that if the domain name was

---

[62] Although some case law suggests that the mere ability to access a website within a jurisdiction, without more, is insufficient basis at least for the assertion of personal jurisdiction against a defendant website operator. See, for example, *Bensusan Restaurant Corp v King*, 937 F Supp 295 (S.D.N.Y. 1996), *aff'd* 126 F 3d 25 (2d Cir 1997) (the defendants who operated a jazz club in Missouri could not be subject to personal jurisdiction in New York by the owners of a jazz club with the same name in New York City in the absence of conduct greater than advertising their Missouri club on their website that was accessible in New York City, although not specifically directed to New York City residents).

registered in California, this would be sufficient grounds for Californian law to apply.[63] However, if this was the case, clever domain name cybersquatters would simply select a domain name registrar not situated in California.[64]

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 Californian 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. 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,[65] later complained about registration of the relevant name, particularly in the context of an election. The bad faith factors in such a dispute procedure could be borrowed to some extent from the Californian PCAA, although they should perhaps be a little broader in order to cover situations where the politician in question has not yet registered any domain names. They should also cover situations where the registrant attempts to sell the domain name to either 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.

D. POLITICAL CYBERSQUATTING, DEFAMATION LAW AND THE RIGHT OF PUBLICITY

1. DEFAMATION

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. These include defamation law, the right of publicity,[66] and some *sui*

---

63 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. § 1125(d)(2)(A).

64 For example, a list of ICANN-accredited domain name registries from all over the world is available at: http://www.icann.org/registrars/accredited-list.html (last viewed on March 14, 2007).

65 Political parties may, in fact, be in a better position than politicians under the UDRP as currently drafted. See *Friends of Kathleen Kennedy Townsend v Birt* (WIPO Case No D2002-0451) (involving Kathleen Kennedy Townsend's name) (last viewed at March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0451.html), ¶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.")

66 Michael Madow, *Personality as Property: The Uneasy Case for Publicity Rights* in PETER YU (ed), INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE, VOLUME 3, TRADEMARK AND UNFAIR COMPETITION, 345, 3451 (2007) (The right to publicity "gives a

generis state legislation such as California's Business and Professions Code.[67] The most obvious tort that deals with a person's reputation is defamation. Defamation generally refers to false statements which damage an individual's reputation.[68] It may, in fact, be a state or federal wrong, depending on the context.[69] Although defamation may be relevant to variations of the conduct described in this article as 'political cyberfraud' – see *infra* – 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. Rather, it removes from the politician's ready accessibility a domain name that the politician might use to make statements in support of her campaign. Thus, defamation 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 possibly have some application to political cybersquatting. The right of publicity has been described as: "the right of an individual to control the commercial use of his or her name, likeness, signature, or other personal characteristics."[70] It has further been likened 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.[71] 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."[72]

To determine whether the right of publicity might have any application in the political cybersquatting context, two fundamental questions have to be answered. The first is whether the registration of a domain name corresponding with a politician's name

---

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.")

67 See § 17525(a), discussed in more detail in Part ___ *infra*.

68 JANET L SILVERBERG, BUSINESS TORTS, 1-6, ¶ 6.01.

69 *id*, 1-6, ¶ 6.01 (Defamation issues have arisen in federal constitutional law since the United States Supreme Court landmark decision in *New York Times v Sullivan*, 376 U.S. 254 (1964)).

70 GILSON, TRADEMARK PROTECTION AND PRACTICE, 1-2, § 2.16[1].

71 *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 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 trademark or celebrity-endorsed products with which they are associated, and can create a formidable competitive advantage.")

72 *Id*. § 2.15[1][b].

for the purposes of commercial profit amounts to a 'commercial exploitation'[73] of the celebrity's name in the manner contemplated by the law. The second is whether politicians are protected by the right of publicity in the context of purely political campaigns, as distinct from other more commercial activities. Neither question has been definitely answered by any state or federal courts or legislatures in the United States. Additionally, the right of publicity is not accepted in all American states,[74] let alone globally, so that is an additional limitation.

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, or are based on, an unauthorized likeness of a famous celebrity.[75] 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, tee-shirt, 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 or not the pop singer, Britney Spears, had authorized the product line, than in the case of a blank web-page utilizing a domain name that corresponds with her name. This is because the goods in question might constitute a line of products that collectors may want to purchase, whereas a blank webpage – or a webpage that is obviously for sale to the highest bidder - is unlikely to attract consumers in this way.

Even if the domain name is regarded as a 'product' that is being 'sold' in the political cybersquatting context, it is not the kind of product sale generally contemplated

---

[73] *Id.*

[74] GILSON, TRADEMARK PROTECTION AND PRACTICE, § 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.")

[75] *Winterland Concessions Co v Creative Screen Design Ltd*, 210 U.S.P.Q. 6 (N.D. Ill 1980) (dealing with rock star names on tee shirts); *Allen v Men's World Outlet Inc*, 679 F Supp 360, U.S.P.Q. 2d 1850 (use of Woddy Allen look alike for clothing store advertisements); *Hoffman v Capital Cities/ABC Inc,* 255 F 3d 1180, 59 U.S.P.Q. 2d 1363 (9th Cir, 2001) (use of digitally manipulated image of Dustin Hoffman in magazine). In this context, celebrity names will often attain a common law trademark status as well: GILSON, TRADEMARK PROTECTION AND PRACTICE, 1-2, § 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 the name or likeness will enjoy the benefits provided by the [Lanham Act]".)

by the right of publicity. It is not really a sale to consumers of an unauthorized celebrity likeness. Rather, it is potentially a sale of a product to an individual who might utilize is it many ways – as an unauthorized fan site in the case of a celebrity or as a site to disseminate information about a politician in the political context. In other words, perhaps political cybersquatting is more like selling the means through which someone may engage in conduct that may or may not be sanctioned by various laws – including political cyberfraud laws.[76] It may thus result in some form of contributory infringement for some other kind of tort but may not in and of itself amount to conduct that would ordinarily be proscribed by the right of publicity.

Even if this analysis is not correct, 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.[77] This question was recently cast into the limelight in a case involving Arnold Schwarzenegger, as governor of California, filing a lawsuit against a manufacturer of bobblehead dolls bearing his name and likeness.[78] Although the case was settled, it raised many issues as to the application of the right of publicity to politicians, as opposed to people whose celebrity is derived from other means.

The issue was particularly confusing in the Governor Schwarzenegger situation because he had attained fame and celebrity through sports, film, and political careers. 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 could be seen as purely usurping the Governor's commercial interests in his persona and likeness.[79]

---

[76] *See* Part ___, *infra*.

[77] See, for example, *Martin Luther King, Jr Center for Social Change, Inc v American Heritage Products, Inc.,* 508 F. Supp. 854 (N.D. Ga. 1981), *rev'd per curiam*, 694 F. 2d. 674 (11th Cir. 1983) (holding that the right of publicity extends to 'public figures who are not public officials' in the sense of holding public office); *New York Magazine v The Metropolitan Transit Authority*, 987 F. Supp. 254 (1997) (holding that then-Mayor Rudolph Guiliani could not succeed in a right of publicity with respect to advertisements for the New York times that depicted him 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 New York Times' First Amendment rights); *New York Magazine v The Metropolitan Transit Authority*, 987 F. Supp. 254, 269 (1997) ("Though the ad as a whole is commercial speech, the advertisement undeniably includes an element of political commentary. It would be anomalous indeed to permit a reprint of a caricature of Guiliani that had appeared in the magazine, but prohibit the Ad at issue which includes speech of public interest."

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

[79] Charles Harder and Henry Self III *Schwarzenegger vs Bobbleheads: The Case for Schwarzenneger*, 45 SANTA CLARA L REV 547, 557 (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); William 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, 597-598 (2005) ("[T]he Schwarzenegger

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.[80] Various suggestions were raised as to why this might be the case. They included: (a) politicians are often not generally concerned with commercial use of their image 'because it is not their typical business';[81] (b) politicians do not wish to invest resources into such claims;[82] (c) politicians want to avoid negative publicity that may arise from such claims[83] partly because they do not want to appear 'humorles or soft-skinned';[84] and, (d) politicians are aware that the sale of products bearing their name or likeness might be protected by the First Amendment.[85]

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

---

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 Hollwyood 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.")

[80] William 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, 597-598 (2005) ([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 of 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 likeness made into a bobblehead doll."); Charles Harder and Henry Self III *Schwarzenegger vs Bobbleheads: The Case for Schwarzenneger*, 45 SANTA CLARA L REV 547, 567 (2005) ("Few courts have had an opportunity to rule on an unauthorized commercial use of a political figure's name or likeness. Politicians typically do not pursue such claims …")

[81] Charles Harder and Henry Self III *Schwarzenegger vs Bobbleheads: The Case for Schwarzenneger*, 45 SANTA CLARA L REV 547, 567-8 (2005).

[82] *id.*, 568.

[83] *id.*

[84] William 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, 583 (2005).

[85] *id.*

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.[86] 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 also lack of success on First Amendment grounds.

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.[87] Assuming that First Amendment concerns

---

[86] Charles Harder and Henry Self III *Schwarzenegger vs Bobbleheads: The Case for Schwarzenneger*, 45 SANTA CLARA L REV 547, 557 (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); William 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, 597-598 (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 Hollwyood 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.") 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: Eileen Rielly, *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.")

[87] Charles Harder and Henry Self III *Schwarzenegger vs Bobbleheads: The Case for Schwarzenneger*, 45 SANTA CLARA L REV 547, 565 (2005) ("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.")

can effectively be dealt with on a case-by-case basis,[88] 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.[89] This would appear to be the case whatever the theoretical basis for the right of publicity – which is still a matter of some controversy even in traditional celebrity-focused right of publicity cases.[90]

If the right of publicity is regarded as being theoretically based on Lockean notions of property,[91] there are good arguments that political figures are just as deserving

---

[88] Charles Harder and Henry Self III *Schwarzenegger vs Bobbleheads: The Case for Schwarzenneger*, 45 SANTA CLARA L REV 547, 557 (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); William 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, 597-598 (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 Hollwyood 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.") 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: Eileen Rielly, *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.").

[89] Eileen Rielly, *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, 1170 (1985) ("Political figures have usually invested much time, money, and effort in building up a public image, just as entertainers have. Few people are simply thrust into the political arena. By their own labors, in a very competitive field, political figures have created publicity value in their names and faces.")

[90] For a summary of the various theoretical arguments posited to support the right of publicity, see Michael Madow, *Personality as Property: The Uneasy Case for Publicity Rights* in PETER YU (ed), INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE, VOLUME 3, TRADEMARK AND UNFAIR COMPETITION, 345, 353-361 (2007) (describing moral, economic, and consumer protection-focused theories underlying the right of publicity).

[91] JOHN LOCKE, THE SECOND TREATISE OF CIVIL GOVERNMENT (1690), Chapter V (Locke's theory of property); *Uhlaender v Henricksen,* 316 F. Supp. 1277, 1282 (D. Minn. 1970) ("It is this court's view

of reaping the rewards of their labors in developing their public personas as celebrities.[92] If the right is based on an associated tort-based concept of unjust enrichment,[93] 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."[94] Even if the right of publicity is regarded as being based in theories of personal privacy, it clearly protects some economic benefits.[95] Certainly, political cybersquatters are contemplating economic benefits when registering domain names corresponding with 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,[96]

---

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.") For a critique of the application of this theory in the right of publicity context, see Michael Madow, *Personality as Property: The Uneasy Case for Publicity Rights* in PETER YU (ed), INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE, VOLUME 3, TRADEMARK AND UNFAIR COMPETITION, 345, 354-355 (2007).

92 Eileen Rielly, *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, 1170 (1985) ("Political figures have usually invested much time, money, and effort in building up a public image, just as entertainers have. Few people are simply thrust into the political arena. By their own labors, in a very competitive field, political figures have created publicity value in their names and faces.")

93 Michael Madow, *Personality as Property: The Uneasy Case for Publicity Rights* in PETER YU (ed), INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE, VOLUME 3, TRADEMARK AND UNFAIR COMPETITION, 345, 355-356 (2007) (describing the case for and against an unjust-enrichment model for the right of publicity).

94 *Zacchini v Scripps-Howard Broadcasting Co*, 433 U.S. 562, 576 (1977) (quoting Kalven, *Privacy in Tort Law – Were Warren & Brandeis Wrong?*, 31 LAW & CONTEMP PROBLS 325, 331 (1966)).

95 GILSON ON TRADEMARK PROTECTION AND PRACTICE, § 2.16[5] (on the distinction between personal and property theories underlying the right of publicity and the relationship of personal remedies to proprietary remedies); Eileen Rielly, *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, 1164-1166 (1985) (describing the derivation of a Lockean property right in this context from a privacy intrusion tort). See also Michael Madow, *Personality as Property: The Uneasy Case for Publicity Rights* in PETER YU (ed), INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE, VOLUME 3, TRADEMARK AND UNFAIR COMPETITION, 345, 360-361 (2007) (describing personal autonomy theories that might explain the right of publicity in terms of personal *freedom*, rather than personal *property*); Mark McKenna, *The Right of Publicity and Autonomous Self-Definition*, 67 U PITT L REV 225 (2005).

96 Eileen Rielly, *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, 1171 (1985) ("Most public servants are not trying to make money from their names while they are in office.")

although some may try to make money from their names and positions to fund a campaign for office.[97] Assuming that most politicians will not make a commercial profit from their personas during the majority of their political lifetime, should they be potentially robbed of the commercial benefits of their names and images after they leave office?[98]

In the electoral context, political cybersquatting activities may chill 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. In the absence of the cybersquatting conduct, the use of the name in the political context would be much less expensive than if a cybersquatter needs to be paid off to secure the use of the name in the electoral context. Thus, the cybersquatter's socially wasteful commercial interests could chill protected First Amendment speech in the absence of some remedy at least for the politician.[99] It may be that the right of publicity is a plausible legal possibility to address such conduct. 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.

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[100] to prevent the sale of the products in

---

[97] 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: *Hillary Rodham Clinton v Michele Dinoia*, Claim Number FA050200041461, March 18, 2005.

[98] Eileen Rielly, *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, 1171 (1985) ("[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 cannot prevent others from exploiting his fame, he will have little ability to market himself when he retires.")

[99] 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.

[100] GILSON ON TRADEMARK PROTECTION AND PRACTICE, § 2.16[6] ("Upon proof of violation of the right of publicity the courts almost always grant injunctive relief. Since the primary purpose of the right of publicity is to prevent the unauthorized use of a person's name and likeness, an injunction may be perfectly tailored to prevent further violation."

question as well as perhaps an account of profits[101] or some other kind of monetary damages.[102] 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. 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 to publicity.

In summary, it is simply not clear whether, or to what extent, the right of publicity might help to potential politician-plaintiffs in a cybersquatting action, at least as currently framed. This 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 a politicians' names; and, (c) questions as to whether the kind of remedies tailored for the right of publicity are really what a plaintiff will want in a political cybersquatting case. Similar problems may well 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

California's Business and Professions Code was revised soon after the enactment of the ACPA at the federal level in order to deal with certain kinds of cybersquatting activities. In August of 2000, the Californian legislature enacted several new sections of the Code to counter these kinds of activities – with a somewhat broader scope than the federal legislation.[103] The new § 17525(a) of the Code provides that:

> 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.

---

[101] *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 account for profits may be awarded.")

[102] *id*., (noting that outside the 'account of profits' area of 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).

[103] 15 U.S.C. §§ 1125(d), 1129.

This prohibition is broader than the personal name provisions of the ACPA[104] in several respects. The first is that it extends protection to a deceased personality as well as to a living person. The second, and more relevant for the purposes of this article, is that the Californian legislation sets out a list of bad faith factors that are somewhat broader than those in the federal legislation.[105] In particular, § 17526(j) of the Californian legislation includes as a bad faith factor: "The intent of a person alleged to be in violation of this article to mislead, deceive, or defraud voters."

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 with the name of a living person without regard to the goods or services of the parties. The real question here would be whether the registrant had an intent to 'mislead, deceive, or defraud voters'. 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. Unlike a person engaging in political *cyberfraud*,[106] 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 infringed § 17525(a) regardless of a failure to satisfy the bad faith test in § 17526(j) on a variety of other grounds. It is important to recognize that the bad faith factors in § 17526 are not intended to be exclusive.[107] Additionally, some of the other bad faith factors in § 17526 may apply to political cybersquatting although not, perhaps, as obviously at first glance as § 17526(j) because they do not focus specifically on the political context. They include:

> "(e) The intent of a person alleged to be in violation of this article 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,

---

104 15 U.S.C. § 1129(1)(A).

105 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. §1125(d)(1)(B)(i). However, those factors may well guide courts in interpreting §1129 as there is no specific guidance as to the meaning of 'bad faith' set out specifically in §1129.

106 See discussion in Part ___, *infra*.

107 The wording of § 17526 itself makes this clear by stating that: "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…" [Thereafter follows the list of bad faith factors.]

> 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 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."

Sub-sections (e) and (f) are borrowed relatively directly from the policies and principles underlying both the ACPA and the UDRP. While they appear potentially to have some application to political cybersquatting, they both relate to trademark concepts – likelihood of confusion[108] in the case of sub-section (e) and bona fide offering of goods or services[109] in the case of sub-section (f). 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.

Sub-section (h) is borrowed directly from the ACPA,[110] which in turn was drafted in response to cases where cybersquatters registered multiple domain names corresponding with well-known trademarks.[111] It may or may not have application in a political cybersquatting case, depending on the circumstances. In fact, in both the

---

[108] 15 U.S.C. § 1114(1)(a)(requiring consumer confusion for registered trademark infringement action); 1125(a)(1)(A)(requiring consumer confusion for common law trademark infringement action).

[109] 15 U.S.C. § 1114(1)(a)(requiring commercial exploitation of relevant goods or services for registered trademark infringement action); 1125(a)(1)(A)(requiring commercial exploitation of relevant goods or services for common law trademark infringement action).

[110] 15 U.S.C. § 1125(d)(1)(B)(i)(VIII) (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…").

[111] Such as the conduct of Mr Dennis Toeppen in the early days of Internet domain name disputes. See Jacqueline Lipton, *Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy*, 40 WAKE FOREST L R 1361, 1370-1371 (2005).

commercial and political context, it is obviously possible for an alleged cybersquatter not to register multiple domain names, hoping instead to make a profit from the auction of just one particularly promising name.

Sub-section (i) might be the most fruitful avenue for a politician concerned about political cybersquatting. The one obvious problem with the section is that it is not clear who is a 'rightful owner' of a relevant domain name and on what theoretical basis. Under modern trademark law it appears to have been assumed in many circumstances, including the passage of the ACPA, that a trademark holder is a 'legitimate holder' 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, § 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.

The Californian Business and Professions Code also currently has the same practical problems for politicians as the PCAA. It is untested state legislation which has not been adopted in other jurisdictions and, while it may serve as a useful "legislative 'laboratory'"[112] on many issues related to cybersquatting, it is not likely to be of much immediate assistance to politicians concerned about this conduct.

E. POLITICAL CYBERSQUATTING: POSSIBLE SOLUTIONS

There are obviously various different avenues that can be pursued by politicians concerned about political cybersquatting, depending on the context of the relevant conduct and the jurisdiction. If, for example, a politician can establish trademark rights in her name, like Senator Clinton has done,[113] she will have more options for reprisal against a cybersquatter, as she might avail herself of the trademark-based provisions of the ACPA[114] or the UDRP, as well as some of the other remedies discussed in the

---

[112] REPORT TO CONGRESS: THE ANTICYBERSQUATTING CONSUMER PROTECTION ACT OF 1999, SECTION 3006 CONCERNING THE ABUSIVE REGISTRATION OF DOMAIN NAMES, (last viewed on March 14, 2007 and available at: http://www.uspto.gov/web/offices/dcom/olia/tmcybpiracy/repcongress.pdf), ¶ IV ("California may serve as a legislative 'laboratory' on [the issue of use of personal names in domain names].")

[113] *Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com* (National Arbitration Forum Claim No. FA0502000414641, March 18, 2005) (last viewed on March 14, 2007 and available at http://www.arb-forum.com/domains/decisions/414641.htm) ("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.")

[114] 15 U.S.C. § 1125(d)(1).

preceding sections. 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.[115] In the absence of a trademark right, other remedies might be available, such as those arising under the 'personal name' provisions of the ACPA,[116] as well as potentially actions under the right of publicity or various state cyberfraud[117] and cybersquatting legislation[118] where available.

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 in which the domain name was registered, as well as on whether the politician can establish a trademark right in her name. 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. Particularly in the context of a presidential election, people all around the United States as well as other countries may want to register domain names corresponding with potential candidates' names with an intent to seek profit from the sale of the names.[119] 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 electoral context which is time-sensitive.

One obvious answer to this problem, and to some other associated problems, would be to legislatively ban *all* forms of cybersquatting. 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 any legitimate use or purpose of the name in the hands of the registrant. This would overlap with the current trademark-based regulations,[120] but that should not be a problem. It would prohibit political cybersquatting as well as other conduct that wastes a potentially valuable resource.[121] Alternatively, one could do the same thing with respect only to

---

115 15 U.S.C. § 1125(a).

116 15 U.S.C. § 1129.

117 For example, California's PCAA: Cal. Elec. Code, 18320-23 (Deering Supp. 2005).

118 For example, California's Business and Professions Code, § 17525(a).

119 See discussion in Steve Friess, *As Candidates Mull '08, Web Sites Are Already Running*, THE NEW YORK TIMES, A13 (November 18, 2006) (noting global reach of this issue).

120 Such as the ACPA and the UDRP.

121 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 with trademarks or personal names, but rather correspond with 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', 'caruniverse.com'. If the registrant registers enough of these variations, she could effectively pre-empt

political cybersquatting, depending on the willingness of relevant regulatory bodies to legislate more or less broadly on the question.

One problem with establishing such legal rules – either generally or specific to the political situation - is precisely how they should be enacted and enforced. This is not necessarily a new question. It was confronted to some extent by the drafters of the ACPA and the UDRP, not to mention the various Californian statutes described above.[122] However, legislation dealing with politician's names or with cybersquatting generally outside the trademark context 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 federal constitutional head of legislative power might support such a regulation. Perhaps the commerce power[123] could be used on the basis that the conduct in question potentially affects communications and commerce[124] across all states. However, this would not necessarily deter cybersquatters from outside the United States engaging in this conduct. It is cheap and easy to register a domain name, even a '.com' domain name, in many different countries outside the United States.[125] Thus, a federal legislative package would require a jurisdictional provision, like the 'in rem' provisions in the ACPA.[126] State legislation, on the other hand, would not raise the federal legislative power issues, but would raise difficulties of creating a statute on which federal legislatures could substantially agree. It may also raise jurisdictional concerns and require in rem provisions in case of domain name registrants situated outside the relevant jurisdiction.

The same may be said of approaches that seek to extend on the current state laws that deal more broadly with bad faith domain name registrations than the ACPA. The

---

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 or thousands, or even millions, of dollars for a relevant domain name instead of the standard registration fee of ten to twenty dollars.

122 Cal. Elec. Code, 18320-23 (Deering Supp. 2005), and Business and Professions Code, § 17525(a).

123 U.S. Constitution, Art 1, § 8, cl. 3 (Congress shall have power: "To regulate Commerce with foreign Nations, and among the several States…").

124 This approach was taken by Judge Wood in *Planned Parenthood Federation of American Inc v Bucci*, 42 U.S.P.Q. 1430 (S.D.N.Y. 1997) (in interpreting the application of the Lanham Act to a domain name dispute, the judge noted that the statute, based on Congress' commerce power, applies to Internet domain name registrations and uses because they are part of interstate commerce both on the basis that websites can provide commercial and informational services in multiple states and on the basis that Internet users constitute a national and international audience who must use interstate telephone lines to access the Internet), 10-12 (LEXIS page references).

125 See, for example, the global list of domain name registries accredited by ICANN at http://www.internic.net/origin.html (last viewed on March 14, 2007).

126 15 U.S.C. § 1125(d)(2)(A)(ii).

two Californian statutes discussed above[127] are obvious examples here. One difficulty with extending these laws would come partly in the substantive drafting of the provisions: that is, clarifying the current gaps in the legislation where political cybersquatting is concerned, such as adding a new 'bad faith' factor to the § 17526 of the Business and Professions Code specifically to cover political cybersquatting. Another problem would arise in terms of the procedural aspects of harmonizing the laws to encompass more jurisdictions. That would raise the same problems discussed in the previous paragraph about federal or harmonized state legislation to prohibit all forms of cybersquatting generally or political cybersquatting specifically. These problems are not impossible to overcome, but they could prove time consuming and expensive, particularly for legislation that has not yet been substantially judicially tested in any state.

An alternative, and perhaps more obvious solution, would be to add specific personal name protections to the UDRP. In other words, where the UDRP is currently limited to protecting trademark-based rights from cybersquatting,[128] it could also be extended to protect personal names against cybersquatting.[129] This could be limited to politician's names or could extend more broadly to celebrities and other public figures.[130] The broader approach would certainly cover some difficult situations that have arisen to date under the UDRP.[131] However, the narrower approach, focused purely on politicians'

---

[127] Cal. Elec. Code, 18320-23 (Deering Supp. 2005), and Business and Professions Code, § 17525(a).

[128] UDRP, clause 4(a)(i) (requiring complainant to establish trademark interest as a requisite element of a UDRP claim).

[129] As considered, but ultimately rejected, in the second WIPO report on the domain name process: WIPO, Second WIPO Internet Domain Name Process: The Recognition of Rights and the Use of Names in the Internet Domain Name System, Sept 3, 2001 (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/processes/process2/report/html/report.html#5), ¶¶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.").

[130] *id.*

[131] Such as 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, for example, *Springsteen v Burgar*, Case No D2000-1532 (WIPO Arb. and Medication Ctr., Admin. Panel Decision, Jan. 5, 2001) (involving Bruce Springsteen's name) (last viewed on march 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1532.html), ¶ 6 ("It is common ground that there is no registered trade mark in the name "Bruce Springsteen". In most jurisdictions where trade marks are filed it would be impossible to obtain a registration of a name of that nature. Accordingly, Mr Springsteen must rely on common law rights to satisfy this element of the three part test. It appears to be an established principle from cases such as Jeanette Winterson, Julia Roberts, and Sade that in the case of very well known celebrities, their names can acquire a distinctive secondary meaning giving rise to rights equating to unregistered trade marks, notwithstanding the non-registerability of the name itself. It should be noted that no evidence has been given of the name "Bruce Springsteen" having acquired a 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. In the view

names might be simpler and less confusing 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 under the UDRP, as currently drafted, than politicians because celebrities are more likely to be able to establish trademark-like rights in their names, given that their names and images are used predominantly for commercial purposes. This may be compared with politicians who may or may not have established commercially valuable personas. A politician who wants to avoid commercialization of her image may thus currently be disadvantaged under the UDRP. The same may be said of a less 'famous' politician who has not yet established a major public persona. An extension of the UDRP rules to cover politicians' personal names would correct these imbalances in the system. Such an extension is also arguably more important at the current time than a specific extension of the UDRP to cover personal names of classes of people outside the political arena.

The main advantages with this approach over federal and state legislation are many. The UDRP procedures are fast, inexpensive and international in scope. 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. The addition of a 'politician's name protection' provision to the UDRP would be a minor drafting change and could be achieved quickly and simply.

III. POLITICAL CYBERFRAUD

A. DISTINGUISHING CYBERFRAUD FROM CYBERSQUATTING

"Political cyberfraud" is defined in this article to include various categories of bad faith content involving registration of a domain name corresponding with a politician's name. It differs from "political cybersquatting" in that it looks to the substantive content of the relevant website in association with the domain name, rather than a simple attempt to sell the domain name. Examples of cyberfraud would include publishing misleading or damaging information on a website about the relevant politician or a fraudulent attempt to raise funds in the name of the politician under a domain name corresponding with the politician's name. The substantive content of a relevant website may or may not be 'legitimate' in a strictly legal sense. However, cyberfraud is concerned with publishing the content in concert with a domain name correspond to a politician's name in a manner that appears to cloak the speech with a misleading sense of authority or truthfulness.

---

of this Panel, it is by no means clear from the UDRP that it was intended to protect proper names of this nature. As it is possible to decide the case on other grounds, however, the Panel will proceed on the assumption that the name Bruce Springsteen is protected under the policy; it then follows that the domain name at issue is identical to that name.")

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 is similar to presumptions that appear to be developing in commercial trademark law with respect to domain names corresponding with well-known trademarks. There is now some authority that 'trademark.com' names will resolve to websites authorized or sponsored by relevant trademark holders.[132]

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. This is why, in many ways, pure cybersquatting will be much easier to regulate than cyberfraud. It will likely be much less contentious and will simply be a way of preserving available forums for political debate and preventing waste of those resources, particularly during elections. 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, and these issues might lend themselves more appropriately to local, rather than global, regulation, again 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. The promulgation of defamatory messages about a politician on a website regardless of the domain name used may well be the subject of a successful defamation action under current law. Attempting to defraud the public and raise money fraudulently under a politician's name (and domain name) would presumably contravene various criminal statutes.[133] Of course, conduct like this arguably has two parts: one is the website content and the other is the unauthorized use of a domain name corresponding with a politician's name. It may be that current defamation and fraud laws cover much of the conduct relating to web content, but that it

---

[132] See discussion in Part ___, *infra*.

[133] 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 Department of Justice, Internet Fraud, last viewed on March 14, 2007 and available at http://www.usdoj.gov/criminal/fraud/Internet.htm). While 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.

is necessary to have additional laws relating to the use of a domain name corresponding to a politician's name in this context.

This might be somewhat akin to the registration of a domain name corresponding with a trademark to promulgate a misleading or deceptive message about the trademark holder. Such conduct has been variously dealt with under current trademark laws. However, it raises additional dimensions in the political context because of the importance of free speech in political discourse. Additionally, it is arguable that legal regulation in the political context, compared with the trademark context, should not be based on the notion of a property-like right in a personal name. While trademarks have clearly attained a property-like status within our legal system,[134] it is not clear that politician's names have achieved a similar status. Even in the context of the right of publicity, it is not clear that politician's names should be treated in the same was as celebrities' names because of the trademark-like status of a celebrity's persona compared to a politician's name and likeness.[135]

In the political context, it is more appropriate for the theoretical basis underlying the protection of a politician's name in a corresponding domain space to reside in notions of democratic government and free speech, rather than in notions of property. 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. This probably accords with voter expectations and is likely the most effective presumption for preserving and facilitating political debate, particularly in an electoral context. However, 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 if the more obvious versions of her name are reserved to Senator Clinton – such as 'hillaryclinton.com'.

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 may be similar. If the social expectations are that the 'rightful' holder of the name is the politician or the trademark-holder, depending on the context, it is possible to draw into the political context some principles

---

[134] Trademarks are often colloquially referred to as 'property' rights although technically they are not 'property' in more traditional senses of the word: Stacey Dogan and Mark Lemley, *Trademarks and Consumer Search Costs on the Internet*, 41 HOUSTON LAW REVIEW 777, 788 (2004) ("trademarks are not property rights in gross, but limited entitlements to protect against uses that diminish the informative value of marks"); Mark Lemley, *The Modern Lanham Act and the Death of Common Sense*, 108 YALE LAW JOURNAL 1687, 1687-1688 (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.").

[135] As noted in Part ___, *supra*, a politician's public persona is often not based on commercial activities, but rather activities in the public service realm.

that have been developed in the trademark context to date. This is not because a politician's rights in her name should necessarily be equated to property rights, although that is possible. 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. Thus, the protection of social expectations 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 a presumption already seems to be developing in domain name disputes that 'trademark.com' names are reserved to legitimate trademark holders, while 'trademarksucks.com' names can be used legitimately for purposes of criticism and commentary consistent with the First Amendment.[136] Thus, the same may be said of political domain names – the 'politicianname.com' version could be reserved to the politician while 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 Californian legislation relating to bad faith registrations and uses of a domain name 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. Although a number of practical procedural problems arise with respect to legislation as opposed to revision of the UDRP, as discussed *supra*,[137] 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 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

---

[136] However, such a presumption is not uniformly accepted. Compare, for example, *Bridgetsone-Firestone v Myers,* Case No, D2000-0190, WIPO Arbitration and Mediation Center, July 6, 2000, (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0190.html), ¶6 ("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."); *Societé Air France v Virtual Dates Inc*, Case No. D2005-0168 (WIPO Arbitration and Mediation Center, May 24, 2005) (majority of arbitration panel found that 'airfrancesucks.com' domain name was sufficiently confusing to consumers to order the name to be transferred to the relevant trademark holder – Air France). 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 CONNECTICUT L R 973 (2007). See also Jacqueline Lipton, *Commerce vs Commentary: Gripe Sites, Parody and the First Amendment in Cyberspace*, WASHINGTON UNIVERSITY L R, forthcoming, 2007.

[137] See discussion in Part ___, *supra*.

Unsurprisingly, California's Political Cyberfraud Abatement Act ("PCAA") appears to be a good legislative model expressly targeted to the kinds of conduct described in this article as 'political cyberfraud'. However, the provisions of the PCAA are intended to be broader than to apply simply to protect domain names corresponding specifically to politician's names from misleading and deceptive uses. Thus, there may be some difficulties and inconsistencies in applying the legislation in this context. The legislation prohibits conduct of the three classes referred to in the previous section: that is, (a) attempts to deny a person access to a political website,[138] (b) attempts to deny a person the opportunity to register a domain name for a political website,[139] and, (c) activities concerning a web site that would cause a person to believe that the website actually represents the views of a proponent or opponent of a ballot measure.[140] Probably classes (b) and (c) are the most relevant to the kind of conduct under consideration here, although some such conduct may arguably fall within class (a).

Class (a) may be less relevant here because if a person registers a domain name corresponding with a polician's name to promulgate a misleading or deceptive message about the politician, she may or may not have actually 'denied the person access to a political website'. The access question would depend upon whether the politician in question still had access to *any* relevant domain names to promulgate her own political message. If the domain name registrant had registered multiple domain names corresponding to the politician'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). However, this may also be regarded as 'cybersquatting' under the relevant cybersquatting regulations, particularly if there is a corresponding attempt to profit from sale of the name. Thus, the cybersquatting laws may deal effectively with access questions in the multiple domain name registration context, and cyberfraud of the kind contemplated in this article could be addressed squarely under classes (b) and (c) of legislation like the PCAA.

Class (b) would obviously cover situations where a person registers a domain name corresponding with a politician's name with a view to denying the politician the opportunity to register that domain name. 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. 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. The legislative phrase 'to deny a person the opportunity to register a domain name for a political Web site'[141] is ambiguous in this context. Does the indefinite article refer to one

---

138 PCAA, § 18320(c)(1).

139 *id*.

140 *id.*

141 *id.*

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 even the less pejorative, but also less intuitive, 'nameinfo.com' or even 'name.info'.

Class (c) may be more promising for victims of the kind of political cyberfraud under discussion in this article. 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. This would clearly contemplate conduct where a person registered a domain name corresponding with a politician's name for the purposes of promulgating a misleading message about the politician's views. Some of these situations may also be caught by defamation law, depending on the content of the website. However, the PCAA may well cast a broader net here and be cheaper and easier to litigate that defamation. 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 with the relevant politician that does not exist. This could be established by proving that the defendant had registered a domain name corresponding with the politician's name to provide messages about the politician regardless of whether the messages were defamatory or not. The 'misleading' conduct would simply be using the politician's name in the domain name for an unauthorized, unofficial website about the politician.[142]

Taking this view of the 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. 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 politician's name in the domain space would not mislead Internet users to think that the site actually reflected the relevant politician's views.

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, as well as cybersquatting in some cases. Such provisions may prove to be an effective complement to defamation laws applied online to the extent that those laws sufficiently protect politicians – and public expectations – against the kind of conduct contemplated here. Because 'cyberfraud' is a somewhat more subjective term than 'cybersqsuatting', 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 protect free speech during an election

---

[142] 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.

campaign in the most effective way possible – in order 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.

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

C. LAWS PROTECTING PERSONAL REPUTATION

Some of the 'personal reputation' laws discussed with respect to political cybersquatting *supra* may also have some application to political cyberfraud. Defamation is an obvious contender here. Also, the right of publicity may have some application, although this seems less likely because of the focus of that right on attempts to use a famous name or likeness to commercialize on the success of another, as opposed to commenting on another. State legislation like California's Business and Professions Code may have some application here, although it is more clearly directed to cybersquatting conduct. As described in the cybersquatting discussion *supra*, § 17525(a) of the Code prohibits the bad faith registration, trafficking or use of a domain name that is identical or confusingly similar to the personal name of another person. This would certainly cover the registration or use of a domain name corresponding with a politician's name for 'bad faith' purposes such as promulgating a misleading message about the politician. Again, it will be task for the judiciary to establish the boundaries of 'bad faith' in this context. 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. They are found in §§ 17526(e), (i) and (j) respectively.

Sub-section 17526(e) contemplates 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." As noted in the preceding discussion, this section is written in trademark-based language with its references to goodwill and likelihood of confusion. However, as also acknowledged above, it is possible to draw some lessons for the political context from trademark presumptions developed in the domain space. 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.

The legislation here is concerned with both profit and consumer confusion motives – which seem to connote both cybersquatting and cyberfraud. 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 or not. Whether or not 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 cybersquatting which only needs to look at the registration of the name and a bad faith attempt to profit from its sale, regardless of website content. Thus, the Business and Professions Code may cover either or both types of conduct depending on the context. It may be that a particular registrant has engaged in both cybersqsuatting and cyberfraud simultaneously, although this will not always be the case. The use of a domain name corresponding letter-for-letter with a politician's name where the website promulgates misleading messages about the politician as well as offering to sell the domain name to the highest bidder would clearly infringe the Code and amount to both cyberfraud and cybersquatting conduct. However, a simple attempt to sell such a name without utilizing any web content about the politician could be prohibited under the legislation *per se* as cybersquatting. On the other hand, the use of the same domain name in concert with content that confuses readers about endorsement by a particular politician[143] could contravene the legislation and amount to cyberfraud.

Sub-section 17526(i) of the Code contemplates as an indicia 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'. If we presume a politician is the 'rightful owner' of a domain name corresponding with her personal name, this provision will certainly cover some cyberfraud. The question will always be context-specific with respect to the domain name actually registered and presumptions about the identity of the 'rightful owner' of that name. While 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 name, this may well chill political speech overall. However, by the same token, there should be some domain space reserved for legitimate political messages to be directly communicated by the relevant politician to the public.

Finally, sub-section 17526(j) of the Code contemplates as a bad faith factor the intent of a domain name registrant 'to mislead, deceive, or defraud voters'. While 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 electoral process content-wise. It must at least implicitly refer to the content of the relevant website and the relationship between web content and the domain name in question.

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

[143] For example, a deliberate misspelling of the politician's name or a 'politiciansucks.com' name.

potentially political cybersquatting. As with provisions of the PCAA, it may be worth watching the interpretation of this legislation and treating California as a laboratory for testing how courts interpret all of this legislation with respect to both political cybersquatting and political cyberfraud. 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. 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, although this could also lead to disharmonization, particularly in the context of a federal election.

D. POLITICAL CYBERFRAUD AND THE ANTI-CYBERSQUATTING REGULATIONS

Other regulations may also overlap in their application to political cyberfraud and political cybersquatting. The regulations aimed directly at cybersquatting, like the ACPA and the UDRP, may well have applications in the cyberfraud area depending on the registrant's conduct. Even though each of these regulatory measures is premised on domain name registration or use with a bad faith profit motive,[144] they may apply to cases of cyberfraud where the profit motive overlaps with misleading or deceptive use of a domain name in a political website. Of course neither of these regulatory measures is likely to apply in the absence of a trademark interest in the politician's name. The one exception to this is the 'personal name' provisions of the ACPA which will protect a person (including a politician) against a bad faith registration of a domain name corresponding with that person's name without that person's consent.[145]

Again, the theoretical basis of the consent requirement is not clear from the legislation. As this is a trademark protection statute, it would seem that the Congressional power being exercised here is the commerce power and it is being used to create commercial property or property-like rights in domain names corresponding with personal names. However, as noted in the previous section, it would seem more theoretically satisfying, at least in the political context, to base any rights in a domain name corresponding to a politician's name on notions of democratic government rather than commercial property. Obviously, the personal name provisions of the ACPA were not drafted with politics in mind, although some domain name arbitrators have suggested that these provisions are the most effective way for a politician who does not have a

---

[144] 15 U.S.C. §§ 1125(d)(1)(a)(i) ("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…"), 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.") (emphases added).

[145] 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.")

trademark interest in her personal name to protect it against unauthorized incursions in the domain space.[146]

The main problem with the personal name provisions in the ACPA[147] is that they will not apply to any kind of cyberfraud unless there is a corresponding cybersquatting motive. In other words, if there is no bad faith intent to sell the domain name in question, the personal name protections in the ACPA will not apply.[148] Thus, if a registrant utilized a domain name corresponding with a politician's name to make comments about the politician, no action would lie unless the registrant had also at some point attempted to sell the domain name to the politician or to someone else.[149] Thus, the ACPA provisions will be limited to cases involving cybersquatting, even if they also involve cyberfraud.[150] As such, they do not add much do a discussion of pure cyberfraud that does not involve such a bad faith profit motive.

The UDRP may be a little different here. Although, like the ACPA, it is premised on notions of bad faith cybersquatting, it is a little broader in its drafting in terms of coverage. 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;[151] (b) has no rights or legitimate interests in the name;[152] and, (c) has registered and used the domain name in bad faith.[153] Unlike an ACPA action, an attempt to actually sell the name[154] – or make some other form of profit

---

146 *Friends of Kathleen Kennedy Townsend v Birt* (WIPO Case No D2002-0451) (involving Kathleen Kennedy Townsend's name) (last viewed at March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0451.html), § 6 ("This does not mean that Complainant is without remedy. The ACPA contains express provisions protecting the rights in personal names.")

147 15 U.S.C. § 1129(1)(A).

148 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)

149 *id.*

150 The same is technically true of the more trademark focused provisions of the ACPA found in 15 U.S.C. § 1125(d). That section is requires a bad faith profit motive, although not necessarily a sale motive. See 15 U.S.C. § 1125(d)(1)(A)(i) (setting out the 'bad faith intent to profit' from a trademark requirement in a trademark-based cybersquatting action, as distinct from the personal name protecting action in 15 U.S.C. § 1129(1)(A)).

151 UDRP, cl. 4(a)(i).

152 UDRP, cl. 4(a)(ii).

153 UDRP, cl. 4(a)(iii).,

154 As required by 15 U.S.C. § 1129(1)(A) with respect to personal names.

from the name in bad faith[155] - is not necessary for a successful UDRP arbitration. The main problem under the UDRP will be for a politician to establish trademark rights in her personal name. If she can establish such rights, then it may be possible to bring a cyberfraud claim under the UDRP if she can prove that the registrant has no legitimate interest in the name and has used it in bad faith.

The next problem would be in establishing the boundaries of 'legitimate' use and 'bad faith' in this context. The UDRP itself gives little guidance here. Although UDRP arbitrators in the past have recognized free speech as a 'legitimate interest',[156] this has occurred in the case of deciding the boundaries of protecting commercial trademark interests.[157] Some have also presumed that free speech will be protected in this context provided that the registrant has not usurped the '.com' version of the name which rightfully belongs to the trademark holder.[158] 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. However, 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.[159] 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.[160] This may

---

155 As required by 15 U.S.C. §1125(d)(1)(A)(i) with respect to trademark-based protections.

156 The UDRP 'legitimate use' factors do not contemplate free speech *per se* and are limited to the various legitimate commercial uses set out in clause 4(c) of the UDRP. This list is not exclusive so arbitrators have had some leeway to extend on it. This occurred in *Bridgetsone-Firestone v Myers,* Case No, D2000-0190, WIPO Arbitration and Mediation Center, July 6, 2000, (last viewed on March 14, 2007 and available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0190.html), ¶6 ("The question presented in this case is whether fair use and free speech are defenses to a claim for transfer of a domain name under the Policy. Under Paragraph 4 (c)(iii) of the Policy, noncommercial fair use is expressly made a defense, as noted above. Although free speech is not listed as one of the Policy's examples of a right or legitimate interest in a domain name, the list is not exclusive, and the Panel concludes that the exercise of free speech for criticism and commentary also demonstrates a right or legitimate interest in the domain name under Paragraph 4 (c)(iii). The Internet is above all a framework for global communication, and the right to free speech should be one of the foundations of Internet law.")

157 *id.* (arbitration involving the Bridgestone-Firestone trademark).

158 *id*., ¶ 6 (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.")

159 *id.*

160 See, for example, *New York Magazine v The Metropolitan Transit Authority*, 987 F Supp 254, 260 (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

thus be a very difficult task to place on the shoulders of UDRP arbitrators who are predominantly trained in commercial trademark law and not constitutional law in any given jurisdiction. In other words, the boundaries of legitimate political speech under the UDRP may be broader than the boundaries of legitimate commercial speech. However, UDRP arbitrators may not be the best arbiters of where the boundaries should lie in the political context.[161]

As with the 'legitimate interests' test under the UDRP,[162] the 'bad faith' use test[163] is drafted in terms of commercial trademark uses such as misleading consumers as to affiliation or source of a particular good or service.[164] The two 'bad faith factors' that may be relevant to political cyberfraud are: (a) 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;[165] and, (b) evidence that the name has been acquired to prevent the trademark holder from reflecting its mark in a corresponding domain name.[166] 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.[167]

E. REGULATING CYBERFRAUD VS REGULATING CYBERSQUATTING

"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.").

[161] Of course, a counter-argument to this is that the UDRP is only intended to protect commercial trademark interests. In the context of protecting trademarks corresponding to politicians' names, maybe UDRP arbitrators are really only being asked the commercial question. However, this could be confusing in practice if the politician in question is really concerned with defamation or other non-commercial reputational damage. It may be better to label such situations as 'pure cyberfraud' situations and litigate them under relevant laws such as defamation or anti-cyberfraud laws, discussed *supra*.

[162] UDRP, cl. 4(c).

[163] UDRP, cl. 4(b).

[164] UDRP, cl. 4(b)(iv).

[165] UDRP, cl. 4(b)(i).

[166] UDRP, cl. 4(b)(ii).

[167] For example, Senator Hillary Clinton in the 'hillaryclinton.com' arbitration: *Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com* (National Arbitration Forum Claim No. FA0502000414641, March 18, 2005) (last viewed on March 14, 2007 and available at http://www.arb-forum.com/domains/decisions/414641.htm) ("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.")

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. In fact, this describes the current regulatory situation. It is a pastiche of laws that generally attempts to regulate all bad faith conduct relating to domain names, political or otherwise. The problem is that these regulations have developed quickly in recent years without close 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. Although both classes of conduct may overlap in some situations, this will not invariably be the case. Political cybersquatting raises issues of wasted political communications channels whereas political cyberfraud deals with fraudulent and misleading uses of a political domain name. Political cybersquatting can thus be regulated fairly simply and mechanically – either a domain name is being used in a wasteful manner or not. A simple arbitration procedure should be able to be implemented to determine this question. On the other hand, political cyberfraud raises substantive questions of speech content in concert with a domain name that are better regulated by those who are experts in balancing legitimate political speech against illegitimate speech. 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 be used somewhat interchangeably.[168] This will likely cause confusions and problems of interpretation of relevant regulations as political campaigns increasingly rely on the Internet and the domain name system in particular.[169] Now may be the time to start unraveling some of the policies underlying the regulation before the confusions become entrenched in the domain name system. Similar confusions have already become entrenched in the system in the purely commercial context, involving the interpretation of the ACPA and the UDRP in trademark-based

---

[168] As noted in the discussion in Part ___, *supra*, California's political cyberfraud legislation, for example, covers aspects of both cyberfraud and cybersquatting. By the same token, anti-cybersquatting regulations such as the ACPA can cover aspects of cyberfraud where they coincide with cybersquatting in practice.

[169] See discussion in Steve Friess, *As Candidates Mull '08, Web Sites Are Already Running*, THE NEW YORK TIMES, A13 (November 18, 2006) (noting importance of use of domain names in future political campaigns, notably the 2008 presidential election).

domain name disputes.[170] This is largely because of a failure to appropriately identify and categorize the competing classes of interests that need to be protected and balanced in the domain name system with respect to trademarks.[171] Similar problems could be avoided in the political context with some regulatory forethought and planning.

III. POLITICIANS' NAMES VS TRADEMARKS

A. "HILLARY.COM": A CASE STUDY

The preceding discussion has argued in favor of identifying two specific categories of bad faith conduct involving domain names corresponding with politician's names – political cybersquatting and political cyberfraud - and with developing appropriate legal responses to them. However, one situation that can arise, albeit rarely, involving political domain names 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 with a politician's name and both parties desire use of a corresponding domain name. An obvious example could arise in the situation of the 'hillary.com' domain name. Many people would think such a name would relate to Senator Hillary Clinton. However, on typing the domain name into a web browser, one would find that the name resolves to a web page administered by a company, Hillary Software Inc, that appears to be a legitimate company with a corresponding trademark or business name.

While this may be confusing in one sense for Internet users looking for the website of Senator Clinton, 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. It is also not an attempt to provide any information about the senator under a relevant domain name. 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 with their business name and trademark and having used the name purely for their own commercial purposes in the software industry.

---

[170] See discussions in Margreth Barrett, *Domain Names, Trademarks, and the First Amendment: Searching for Meaningful Boundaries*, 39 CONNECTICUT L R 973 (2007); Jacqueline Lipton, *Commerce vs Commentary: Gripe Sites, Parody and the First Amendment in Cyberspace*, forthcoming, WASHINGTON UNIVERSITY L R, 2007; Jacqueline Lipton, *Beyond Cybersquatting: Taking Domain Names Past Trademark Policy*, 40 WAKE FOREST L R 1361 (2005).

[171] Jacqueline Lipton, *Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy*, 40 WAKE FOREST L R 1361, 1364 (2005) ("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.")

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. This will be the case whether or not Senator Clinton is regarded as having a trademarked or trademarkable personal name.[172] In any event, trademarked or not, and registered as a mark or not, Senator Clinton could not likely establish trademark infringement[173] by Hillary Software because of the lack of consumer confusion.[174] It is unlikely that web users looking for information about Senator Clinton and her policies would think that the Hillary Software website had anything to do with her. It is possible she might argue 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.[175] However, 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 from Senator Clinton's actual website.

Senator Clinton would additionally be unlikely to establish an infringement of the ACPA provisions protecting personal names[176] because such an action would require that

---

[172] Generally, personal names are not registrable as trademarks: 15 U.S.C. § 1052 (c). See also GILSON ON TRADEMARK PROTECTION AND PRACTICE, ¶ 2.03[d]. However, even unregistered marks can in some cases attain a common law trademark status. In fact, 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 which corresponded to the 'hillaryclinton.com' domain name: National Arbitration Forum, *Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com* (Claim No. FA0502000414641, March 18, 2005). The arbitrator ordered a transfer of the name to Senator Clinton largerly on this basis. 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'.

[173] 15 U.S.C. § 1125 (a)(1).

[174] 15 U.S.C. § 1125 (a)(1)(A). This is perhaps similar to the results that occur in cases involving competing legitimate interests in trademarks where only one associated domain name is available. See, for example, *Hasbro, Inc v Clue Computing Inc*, 66 F Supp 2d 117 (D. Mass. 1999) in which Hasbro failed to show consumer confusion for trademark infringement purposes with respect to the use of the 'clue.com' domain name registered to a company called 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.

[175] 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, for example, *Brookfield Communications Inc v West Coast Entertainment Corp*, 174 F 3d 1036, 1054-1064 (9th Cir 19999); Eric Goldman, *Deregulating Relevancy in Internet Trademark Law*, 54 EMORY LAW JOURNAL 507, 559 ('[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."; *Panavision Int'l v Toeppen*, 141 F 3d 1316 (9th Cir., 1998) (consumers would not actually have been confused as to source by defendant's website, but may have been distracted from finding the plaintiff's actual web presence).

[176] 15 U.S.C. § 1129(1)(A).

the corresponding domain name had been 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'.[177] Assuming that Hillary Software did not register its 'hillary.com' name for this purpose, it is unlikely to run afoul of this provision.

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.[178] In particular, the registrant appears to be using the domain name in connection with a bona fide offering of computer software services.[179] For similar reasons, it is unlikely that Hillary Software has run afoul of the various state laws, notably the California laws, relating to unfair business practices[180] and political cyberfraud,[181] assuming of course these laws could apply to Internet conduct affecting a New York senator. If there is no bad faith for the purposes of the unfair business laws[182] and no willful intent to deceive electors under the cyberfraud legislation,[183] these actions would not likely succeed. Further, 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 be unlikely to succeed.[184]

It is possible that Senator Clinton could succeed in a trademark dilution action,[185] presuming she has a trademark interest here.[186] Such an action is premised on the notion of tarnishment or blurring of a mark.[187] In other words, decreasing the ability of a mark

---

177 15 U.S.C. § 1129(1)(A).

178 UDRP, ¶4(c).

179 UDRP, ¶4(c)(i).

180 California's Business and Professions Code, § 17525(a).

181 Cal. Elec. Code, §§ 18320-23 (Deering Supp. 2005).

182 California's Business and Professions Code, § 17525(a).

183 Cal. Elec. Code, §§ 18320-23 (Deering Supp. 2005).

184 This 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 discussion in Part ___ *supra*.

185 15 U.S.C. §§1125(c)(1), 1127.

186 Although personal names are not generally trademarkable (GILSON ON TRADEMARK PROTECTION AND PRACTICE, ¶ 2.03[d]), a UDRP panel did find the senator to have a common law trademark interest in 'Hillary Clinton': *Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com* (Claim No. FA0502000414641, March 18, 2005). It is not clear whether this would extend to protection of 'Hillary' 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.

187 15 U.S.C. §§1125(c)(1), 1127.

to operate as a mark and identify relevant goods and services. The problem with dilution law is that it is premised on the notion that the underlying mark be famous[188] and be used in connection with the sale of goods or services.[189] It is not clear that Senator Clinton's personal name would qualify on either count, although it is possible.

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[190] 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,[191] or at least lack of bad faith in the registration and use of the name.

This practical 'get in first' solution would remedy potential cyberfraud and cybersquatting concerns as well. However, it is obviously not very practical. 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.[192] For another thing, politicians do not always want to advertise their prospective political ambitions with such registrations – as registration information is generally publicly available on 'whois' searches.[193]

---

188 *id.*

189 *id.*

190 See discussion in Steve Friess, *As Candidates Mull '08, Web Sites Are Already Running*, THE NEW YORK TIMES, A13 (November 18, 2006).

191 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 which corresponded to the 'hillaryclinton.com' domain name: National Arbitration Forum, *Hillary Rodham Clinton v Michele Dinoia a/k/a SZL.com* (Claim No. FA0502000414641, March 18, 2005). The arbitrator ordered a transfer of the name to Senator Clinton largerly on this basis. 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'.

192 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 is apparently registered to a Mr Brett Maverick of Canberra, Australia (Steve Friess, *As Candidates Mull '08, Web Sites Are Already Running*, THE NEW YORK TIMES, A13 (November 18, 2006)) and 'hrc2008.com' which is currently registered to a company called Address Creation, LLC – which may well be a cybersquatter (see http://www.whois.net/whois_new.cgi?d=hrc2008.com&tld=com, last viewed on March 15, 2007).

193 See, for example, 'WHOIS.NET' which is a database of domain name registry information (last viewed on March 15, 2007 and available at http://www.whois.net/).

B. POLITICIANS VS LEGITIMATE TRADEMARK OWNERS: POSSIBLE SOLUTIONS

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.[194] This 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. The difference would be that it 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. It would also need 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, so this would be some compensation for losing the commercial use of the name and may deter politicians from arbitrating for names they do not really need. However, 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.[195] At this point, should she be forced to buy the name from the trademark holder for a reasonable market price?[196]

In any event, even without a licensing system in place, these kinds of disputes would likely only arise in rare cases and some politicians may not care about all commercial registrations of domain names corresponding with their personal names provided that relevant websites do not include any misleading comments about their campaigns and that other intuitive domain names are available for their campaigns.

---

[194] Jacqueline Lipton, *Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy*, 40 WAKE FOREST LR 1361, 1433-1435 (suggesting a compulsory licensing scheme or domain name sharing scheme for political domain names).

[195] For example, Senator John Kerry has maintained his johnkerry.com website (last viewed on March 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.

[196] Jacqueline Lipton, *Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy*, 40 WAKE FOREST L R 1361, 1434 (2005) (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.")

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 as long as they do not allow that name to be used for purposes that might impugn her campaign messages in a misleading way, and provided that she herself can use another equally intuitive domain name such as 'hillaryclinton.com'.

Another potential solution for the rare case of a conflict between a trademark holder and a politician over a domain name could be a 'domain name sharing' order. This could be achieved in exactly the same procedural manner as the domain name licensing arrangement suggested *supra*, but the administrative order could require the politician and the trademark holder to share the relevant domain name rather than for the trademark holder to license it to the politician. This would be an arrangement under which the domain name in question resolved 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. This kind of arrangement is technologically possible with current Internet technologies and may create a fairer and more 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 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 private citizen shared a name like Chris Dodd or Joe Biden with a politician. 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[197] and personal names,[198] as is the UDRP.[199] 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. 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.

IV. CONCLUSIONS AND FUTURE DIRECTIONS

---

197 15 U.S.C. § 1125(d)(1)(A)(i).

198 15 U.S.C. § 1129(1)(A).

199 UDRP, clause 4(a), 4(c)(ii).

The use of domain names and associated web content will increase in the political context in coming years. The Internet is an unprecedented communications medium in terms of being an incredibly low cost method of reaching a tremendously large audience. 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 faced by politicians in terms of bad faith conduct involving Internet domain names will also magnify. 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 thought has been given to questions of domain name regulation in the context of commercial trademark disputes,[200] 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 part of a larger picture about regulating the Internet more broadly. There are several answers to this. While 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 our 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 our system. The need for electors and politicians to have every chance to fully participate 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 advocated in this article to political domain name regulation. Some would argue that focusing on the regulation of domain names at all 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.[201] While this may well be true as a general proposition, this argument only

---

[200] Margreth Barrett, *Domain Names, Trademarks, and the First Amendment: Searching for Meaningful Boundaries*, 39 CONNECTICUT L R 973 (2007); Jacqueline Lipton, *Commerce vs Commentary: Gripe Sites, Parody and the First Amendment in Cyberspace*, forthcoming, WASHINGTON UNIVERSITY L R, 2007; Jacqueline Lipton, *Beyond Cybersquatting: Taking Domain Names Past Trademark Policy*, 40 WAKE FOREST L R 1361 (2005).

[201] Eric Goldman, *Deregulating Relevancy in Internet Trademark Law*, 54 EMORY L J, 507, 548 (2005) ("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.")

considers one perspective – the ability of sophisticated search engines to find information as a result of a particular search query. In other words, while search engines clearly assist with information location, regardless of domain name, they do not necessarily help with the *identificatory* function played by many Internet domain names.

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. The other is to serve almost as a label to *identify* the work.[202] This enables people to refer to the relevant work (or, in the domain name case, web page) by name when talking to others about it. 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.[203] Even when search engines are used to locate a relevant web page, 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.[204] This is further evidence that the actual domain name retains its importance even when users increasingly rely on search engines to locate web content. Additionally, even in the search engine context, many search engines will prioritize web pages with relevant domain names, depending on the search algorithms used. Thus, domain names will retain their importance, despite the rise of increasingly sophisticated search engine technologies.

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. However, to date, 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 a part of incidentally resolving some other domain name questions relating to the protection of personal names in the

---

[202] Jacqueline Lipton, *Commerce vs Commentary: Gripe Sites, Parody and the First Amendment in Cyberspace*, forthcoming, WASHINGTON UNIVERSITY L R, 2007.

[203] Although, ironically, it was not so easy for Vice President Cheney to refer to this website in the Vice Presidential debate in the lead-up to the 2004 presidential election. 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 Harry Chen, *Is the Domain Name .Com or .Org? Dick Cheney was Confused*, HARRY CHEN THINKS ALOUD (last viewed on March 13, 2007 and available at: http://harry.hchen1.com/2004/10/06/89).

[204] Eric Goldman, *Deregulating Relevancy in Internet Trademark Law*, 54 EMORY L J, 507, 548 (2005) ("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.")

domain space more generally.[205] The ACPA provisions relating to the protection of personal names against bad faith cybersquatting[206] are a good example of a law concerned with a broader question that may incidentally protect some politician's names against certain classes of bad faith conduct online. 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.[207] Domain name conflicts involving politicians' names and campaigns may require more speedy attention than has been the case 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.

There are undoubtedly problems relating to domain names in politics that have not been canvassed in any detail within this article. Intentional 'mis-spellings' of politician's names within domain names, for example, have only been incidentally addressed here. This is because they largely raise the same issues as accurate spellings of politicians' names in the domain space and should be separated out into relevant categories of conduct as such. A deliberate misspelling of Senator 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.[208] 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 politician's names in the domain space against various forms of bad faith conduct. Current regulatory measures focusing largely, as they do, on protecting commercial trademark interests in cyberspace do not effectively facilitate 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

---

[205] 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 discussion in Part ___ *supra*.

[206] 15 U.S.C. § 1129(1)(A). See discussion in Part ___ *supra*.

[207] Such as the ACPA, the PCAA and California's Business and Professions Code, § 17525(a).

[208] At the date of writing 'barackobama.com' seems to be registered legitimately to Senator Obama's campaign, while 'barakobama.com' appears to be unregistered.

attempted to do, and then to moot 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.